Cisco Secure Network Analytics

Security Events and Alarm Categories 7.5.1

Table of Contents

Introduction

Overview

This document provides descriptive lists of the security events and alarm categories that you may see in the Manager (formerly Stealthwatch Management Console).

Audience

This document is intended to be used as a reference for network administrators and security personnel responsible for using the Manager to manage and secure their networks.

Related Information

You can find this information also in the Web App Help under the following topics:

- Security Event List
- About Alarm Categories

Acronyms

This document uses the following terms and their acronyms.

Acronym	Term
ASA	Adaptive Security Appliance
CI	Concern Index
DNS	Domain Name System (Service or Server)
DoS	Denial of Service
dvPort	Distributed Virtual Port
ESX	Enterprise Server X
FSI	File Sharing Index
FTP	File Transfer Protocol
ICMP	Internet Control Message Protocol

Acronym	Term
IDS	Intrusion Detection System
IP	Internet Protocol
IRC	Internet Relay Chat
ISE	Identity Services Engine
MAC	Media Access Control
NAT	Network Address Translation
NTP	Network Time Protocol
OS	Operating System
OVF	Open Virtualization Format
RAID	Redundant Array of Independent Discs
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TI	Target Index
UDP	User Datagram Protocol
VDS	Virtual Network Distributed Switch
VE	Virtual Edition
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network

Security Event List

A security event is an algorithm that looks for specific behavior and can alert on that behavior on your network, depending on settings applied in policies. It does this by directly generating a host alarm (if set to do so), or by assigning index points to alarm categories, which can in turn trigger a host alarm. (A host alarm is a security event that has triggered an alarm.)

Security events contribute index points for specific alarm categories. If you disable a security event, it will not accumulate index points against the alarm categories associated with it. Both alarm categories and security events can trigger host alarms, depending on settings applied in policies.

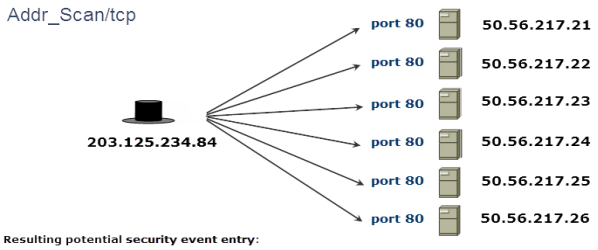
Security events can be disabled for specific services and disabled at the host group level.

- We are currently in the process of updating and expanding security event information. The new format includes information (presented in several tables) such as event description, what it means when an event is triggered, the steps you should take to investigate further, and much more. During this transition, some security events in this topic will contain more completed categories or tables than others.
- The Flow Collector (NetFlow) supports the security events marked with a double asterisk (**) only when it is used in conjunction with a Flow Sensor.

Cisco Secure Network Analytics (formerly Stealthwatch) contains the following default security events.

Addr (Address) Scan/tcp

Mitigation is not available for the alarm associated with this security event.



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope Corporate	50.56.217.21	<CI value>*	Addr_Scan/tcp-80(6)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	If Secure Network Analytics detects activity that potentially indicates someone doing a network scan using TCP, the system records this as a scanning event. If enough scanning events affect a large enough number of hosts, the Manager (formerly Stealthwatch Management Console) raises a security event. Examples of "scanning events" include various combinations of bad TCP flags, or sending a SYN but not responding to the following SYN-ACK, as well as other indicators.
What does it mean when it triggers?	A host is attempting to discover which hosts are running particular services to potentially make use of.
What are next steps?	Determine what the host was scanning. Start this investigation with a broad net and then narrow it down. Begin by running a Top Ports (outbound) report. Set the time period to the day of the event and the client host to be the source IP of the event. Regardless of the target IP range that is listed, you can scan any type of

Questions about this event	Response
	host, so determine if you want to search on Inside Hosts, Outside Hosts, or both. Then, in the Filter dialog, set the Server filter as appropriate on the Hosts tab and set the "Order the records returned by" to *Flows* on the Advanced tab. Once the results come back, it may be helpful to sort by Peers. Regardless, start at the top of the list as sorted by Flows or Peers to find the standout ports that either don't belong or appear abnormally high. Right-click an IP address to pivot to the flows to view the various IP addresses and determine if particular host groups are those being primarily targeted. You can also right-click and pivot to the Top Peers report to determine whether or not the traffic is spread generally equally across the targets. It is also worth noting the percentage of hosts that responded to the scans. At this point you should be able to determine who the host was scanning and what ports were being scanned.
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	Some scans are only recorded based on flags sent by the FlowSensor, and some by flags sent by firewalls. (These are noted in the event details). Scanning events that are not noted as such do not require any specific data.
Notes	N/A

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	Event must be enabled on the source host

Questions about event	Response
Which policies have this event on by default?	Inside Hosts, Outside Hosts, Client IP Policy
Which policies have this event off by default?	Antivirus & SMS Servers; Firewalls, Proxies, & NAT Devices; Network Management & Scanners
Which policies have this alarm on by default?	None
Which policies have this alarm off by default?	Inside Hosts, Outside Hosts, Client IP Policy; Antivirus & SMS Servers; Firewalls, Proxies, & NAT Devices; Network Management & Scanners
Can you tune this event?	No
Is the event variance-based, threshold-based, or other?	N/A
What are default values and units?	
Tolerance	N/A
Minimum threshold value	N/A
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A
Is event tunable outside of the normal policy editor	Yes
If so, what are the alternate locations of tunable values?	You can use the disable_stealth_probe lc_threshold.txt value to disable certain cases of stealth scan detection.

Questions about event	Response
Does event have a default mitigation?	No
If so, what is it?	N/A

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host performing the activity that may be an indication of scanning
What is the target?	The host being scanned by the source host.
Which policy causes the event to trigger?	The source host
What alarm categories does this security event contribute to for the source?	High Recon Index, High Concern Index
In what quantity?	• High Recon Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed	Manager: View details.

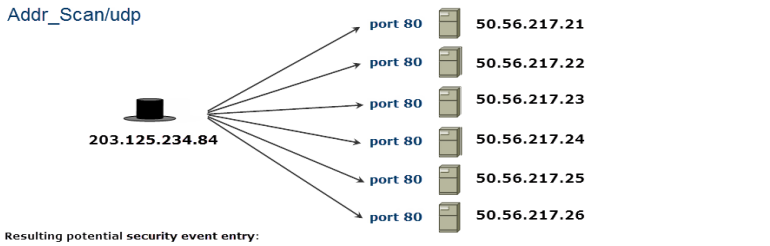
Questions about event	Response
in the alarm details?	Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source IP, the target's natural class C network (/24), the start time (reset hour) of the event's active day until the event's last active time, and TCP. Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_TCP_ADDR_SCAN (276)

Addr (Address) Scan/udp

Mitigation is not available for the alarm associated with this security event.



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope Corporate	50.56.217.21	<CI value>*	Addr_Scan/udp-80(6)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	If Secure Network Analytics detects activity that potentially indicates someone doing a network scan using UDP, the system records this as a scanning event. If enough scanning events affect a large enough number of hosts, the Manager raises a security event. Examples of "scanning events" include sending UDP packets that are responded to by various type of ICMP rejections or firewall flow- denied messages, among other indicators.
What does it mean when it triggers?	A host attempting to discover which hosts are running particular services to potentially make use of.
What are next steps?	Determine what the host was scanning. Start this investigation with a broad net and then narrow it down. Begin by running a Top Ports (outbound) report. Set the time period to the day of the event and the client host to be the source IP of the event. Regardless of the target IP range that is listed, you can scan any type of host, so determine if you want to search on Inside

Questions about this event	Response
	Hosts, Outside Hosts, or both. Then, in the Filter dialog, set the Server filter as appropriate on the Hosts tab and set the "Order the records returned by" to *Flows* on the Advanced tab. Once the results come back, it may be helpful to sort by Peers. Regardless, start at the top of the list as sorted by Flows or Peers to find the standout ports that either don't belong or appear abnormally high. Right-click an IP address to pivot to the flows to view the various IP addresses and determine if particular host groups are those being primarily targeted. You can also right-click and pivot to the Top Peers report to determine whether or not the traffic is spread generally equally across the targets. It is also worth noting the percentage of hosts that responded to the scans. At this point you should be able to determine who the host was scanning and what ports were being scanned.
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	Some scans are only recorded based on flags sent by the FlowSensor, and some by flags sent by firewalls. (These are noted in the event details). Scanning events that are not noted as such do not require any specific data.
Notes	N/A

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	Event must be enabled on the source host
Which policies have this event	Inside Hosts, Outside Hosts, Client IP Policy

Questions about event	Response
on by default?	
Which policies have this event off by default?	Antivirus & SMS Servers; DHCP Server; Firewalls, Proxies, & NAT Devices; Network Management & Scanners
Which policies have this alarm on by default?	None
Which policies have this alarm off by default?	Inside Hosts, Outside Hosts, Client IP Policy; Antivirus & SMS Servers; DHCP Server; Firewalls, Proxies, & NAT Devices; Network Management & Scanners
Can you tune this event?	No
Is the event variance-based, threshold-based, or other?	N/A
What are default values and units?	N/A
Tolerance	N/A
Minimum threshold value	N/A
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A
Is event tunable outside of the normal policy editor	Yes
If so, what are the alternate locations of tunable values?	You can use the disable_stealth_probe lc_threshold.txt value to disable certain cases of stealth scan detection.

Questions about event	Response
Does event have a default mitigation?	N/A
If so, what is it?	N/A

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host performing the activity that may be an indication of scanning
What is the target?	The host being scanned by the source host.
Which policy causes the event to trigger?	The source host
What alarm categories does this security event contribute to for the source?	High Recon Index, High Concern Index
In what quantity?	• High Recon Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed	Manager: View details.

Questions about event	Response
in the alarm details?	Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source IP, the target's natural class C network (/24), the start time (reset hour) of the event's active day until the event's last active time, and UDP. Desktop Client: Flows are filtered by time period of last five minutes.

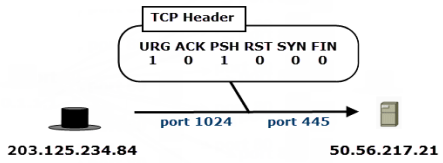
What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_UDP_ADDR_SCAN (286)

Bad Flag ACK (Acknowledge) **

Mitigation is not available for the alarm associated with this security event.

Bad_Flag_ACK



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope Corporate	50.56.217.21	<CI value>*	Bad_Flag_ACK-445(1)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	If a packet is seen not containing the TCP acknowledge flag and containing any flag besides reset or synchronize, the security event is triggered on the originating host.
What does it mean when it triggers?	A TCP packet with invalid flags set should not normally happen. When it does happen, it has likely been done intentionally in an attempt to gather information about the machine to which the packet is sent since different system configurations may respond to different anomalous flag combinations differently.
What are next steps?	If the source of this event is an inside host, it is worth looking for other signs of recon activity. For example, is the host sending bad flag combinations to multiple hosts? Is it scanning many hosts on the same port? Is it scanning many ports on one host? An inside host performing reconnaissance can be a good sign of unwanted activity or compromise.
Non-standard flow data required?	For Flow Collector NetFlow edition, a FlowSensor is required. For Flow Collector sFlow, no special extras

Questions about this event	Response
(FlowSensor, proxy, firewall, etc.)	are required.
Notes	N/A

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	Enable Security event Bad_Flag_ACK on the originating host.
Which policies have this event on by default?	Inside Hosts, Outside Hosts, Client IP Policy
Which policies have this event off by default?	Antivirus & SMS Servers; Firewalls, Proxies, & NAT Devices; Network Management & Scanners
Which policies have this alarm on by default?	None
Which policies have this alarm off by default?	Inside Hosts; Outside Hosts; Client IP Policy; Antivirus & SMS Servers; Firewalls, Proxies, & NAT Devices; Network Management & Scanners
Can you tune this event?	No
Is the event variance-based, threshold-based, or other?	N/A
What are default values and units?	
Tolerance	N/A

Questions about event	Response
Minimum threshold value	N/A
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	N/A
If so, what is it?	N/A

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host that sent the bad packet
What is the target?	The host listed as the bad packet's destination
Which policy causes the event to trigger?	The source's host policy
What alarm categories does this security event contribute to for the source?	High Recon Index, High Concern Index

Questions about event	Response
In what quantity?	• High Recon Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: View details. Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source & target IP, a time range five minutes before the event's first active time until the event's last active time, the associated port as <port>/TCP and <port>/UDP, and TCP. Desktop Client: Flows are filtered by time period of last five minutes.

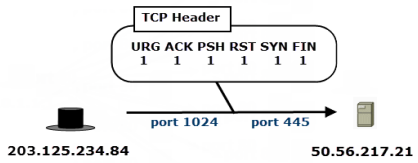
What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_BAD_FLAG_NO_ACK (267)

Bad Flag All **

Mitigation is not available for the alarm associated with this security event.

Bad_Flag_All



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope Corporate	50.56.217.21	<CI value>*	Bad_Flag_All-445(1)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	If a packet is observed containing all of the TCP flags (synchronize, acknowledge, reset, push, urgent, and finish), the security event is triggered on the originating host.
What does it mean when it triggers?	A TCP packet with all flags set should not normally happen. When it does happen, it has likely been done intentionally in an attempt to gather information about the machine to which the packet is sent since different system configurations may respond to different anomalous flag combinations differently.
What are next steps?	If the source of this event is an inside host, it is worth looking for other signs of recon activity. For example, is the host sending bad flag combinations to multiple hosts? Is it scanning many hosts on the same port? Is it scanning many ports on one host? An inside host performing reconnaissance can be a good sign of unwanted activity or compromise.
Non-standard flow data required?	For Flow Collector NetFlow edition, a FlowSensor is required. For Flow Collector sFlow, no special extras

Questions about this event	Response
(FlowSensor, proxy, firewall, etc.)	are required.
Notes	N/A

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	Enable Security event Bad_Flag_All on the originating host.
Which policies have this event on by default?	Inside Hosts, Outside Hosts
Which policies have this event off by default?	N/A
Which policies have this alarm on by default?	Inside Hosts, Outside Hosts
Which policies have this alarm off by default?	N/A
Can you tune this event?	No
Is the event variance-based, threshold-based, or other?	N/A
What are default values and units?	
Tolerance	N/A
Minimum threshold value	N/A

Questions about event	Response
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	N/A
If so, what is it?	N/A

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host that sent the bad packet
What is the target?	The host listed as the bad packet's destination
Which policy causes the event to trigger?	The source's host policy
What alarm categories does this security event contribute to for the source?	High Recon Index, High Concern Index
In what quantity?	• High Recon Index: True

Questions about event	Response
	• CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: View details. Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source & target IP, a time range five minutes before the event's first active time until the event's last active time, the associated port as <port>/TCP and <port>/UDP, and TCP. Desktop Client: Flows are filtered by time period of last five minutes.

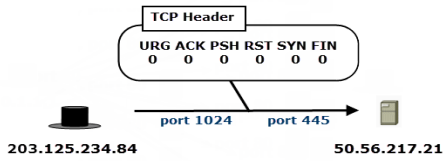
What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_BAD_FLAG_XMAS (263)

Bad Flag NoFlg **

Mitigation is not available for the alarm associated with this security event.

Bad_Flag_NoFlg



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope Corporate	50.56.217.21	<CI value>*	Bad_Flag_NoFlg-445(1)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	If a packet is seen containing no TCP flags, the security event is triggered on the originating host.
What does it mean when it triggers?	A TCP packet with invalid flags set should not normally happen. When it does happen, it has likely been done intentionally in an attempt to gather information about the machine to which the packet is sent since different system configurations may respond to different anomalous flag combinations differently.
What are next steps?	If the source of this event is an inside host, it is worth looking for other signs of recon activity. For example, is the host sending bad flag combinations to multiple hosts? Is it scanning many hosts on the same port? Is it scanning many ports on one host? An inside host performing reconnaissance can be a good sign of unwanted activity or compromise.
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	For Flow Collector NetFlow edition, a FlowSensor is required. For Flow Collector sFlow, no special extras are required.

Questions about this event	Response
Notes	N/A

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	Enable Security event Bad_Flag_NoFlg on the originating host.
Which policies have this event on by default?	Inside Hosts, Outside Hosts, Client IP Policy
Which policies have this event off by default?	Antivirus & SMS Servers; Firewalls, Proxies, & NAT Devices; Network Management & Scanners
Which policies have this alarm on by default?	None
Which policies have this alarm off by default?	Inside Hosts; Outside Hosts; Client IP Policy; Antivirus & SMS Servers; Firewalls, Proxies, & NAT Devices; Network Management & Scanners
Can you tune this event?	No
Is the event variance-based, threshold-based, or other?	N/A
What are default values and units?	
Tolerance	N/A
Minimum threshold value	N/A
Maximum threshold value	N/A

Questions about event	Response
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	N/A
If so, what is it?	N/A

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host that sent the bad packet
What is the target?	The host listed as the bad packet's destination
Which policy causes the event to trigger?	The source's host policy
What alarm categories does this security event contribute to for the source?	High Recon Index, High Concern Index
In what quantity?	• High Recon Index: True • CI: True

Questions about event	Response
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: View details. Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source & target IP, a time range five minutes before the event's first active time until the event's last active time, the associated port as <port>/TCP and <port>/UDP, and TCP. Desktop Client: Flows are filtered by time period of last five minutes.

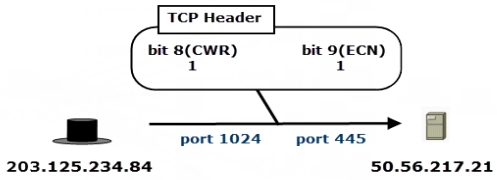
What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_BAD_FLAG_NOFLAG (269)

Bad Flag Rsrvd (Reserved)

Mitigation is not available for the alarm associated with this security event.

Bad_Flag_Rsrvd



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope Corporate	50.56.217.21	<CI value>*	Bad_Flag_Rsrvd-445(1)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	If a packet is seen containing TCP flags that were reserved in the initial TCP standard, the security event is triggered on the originating host.
What does it mean when it triggers?	A TCP packet with invalid flags set should not normally happen. When it does happen, it has likely been done intentionally in an attempt to gather information about the machine to which the packet is sent since different system configurations may respond to different anomalous flag combinations differently.
What are next steps?	If the source of this event is an inside host, it is worth looking for other signs of recon activity. For example, is the host sending bad flag combinations to multiple hosts? Is it scanning many hosts on the same port? Is it scanning many ports on one host? An inside host performing reconnaissance can be a good sign of unwanted activity or compromise.
Non-standard flow data required?	Flow Collector NetFlow edition will never trigger this event. For Flow Collector sFlow, no special extras are

Questions about this event	Response
(FlowSensor, proxy, firewall, etc.)	required.
Notes	N/A

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	Enable Security event Bad_Flag_Rsrvd on the originating host.
Which policies have this event on by default?	Inside Hosts, Outside Hosts, Client IP Policy
Which policies have this event off by default?	Antivirus & SMS Servers; Firewalls, Proxies, & NAT Devices; Network Management & Scanners
Which policies have this alarm on by default?	None
Which policies have this alarm off by default?	Inside Hosts; Outside Hosts; Client IP Policy; Antivirus & SMS Servers; Firewalls, Proxies, & NAT Devices; Network Management & Scanners
Can you tune this event?	No
Is the event variance-based, threshold-based, or other?	N/A
What are default values and units?	
Tolerance	N/A

Questions about event	Response
Minimum threshold value	N/A
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	N/A
If so, what is it?	N/A

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host that sent the bad packet
What is the target?	The host listed as the bad packet's destination
Which policy causes the event to trigger?	The source's host policy
What alarm categories does this security event contribute to for the source?	High Recon Index, High Concern Index

Questions about event	Response
In what quantity?	• High Recon Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: View details. Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source & target IP, a time range five minutes before the event's first active time until the event's last active time, the associated port as <port>/TCP and <port>/UDP, and TCP. Desktop Client: Flows are filtered by time period of last five minutes.

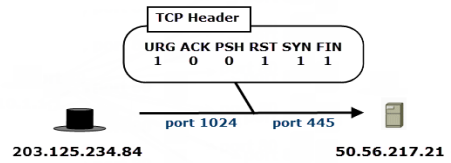
What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_BAD_FLAG_RESERVED (265)

Bad Flag RST (Reset) **

Mitigation is not available for the alarm associated with this security event.

Bad_Flag_RST



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope Corporate	50.56.217.21	<CI value>*	Bad_Flag_RST-445(1)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	If a packet is seen containing the TCP reset and any other flags besides push or acknowledge, the security event is triggered on the originating host.
What does it mean when it triggers?	A TCP packet with invalid flags set should not normally happen. When it does happen, it has likely been done intentionally in an attempt to gather information about the machine to which the packet is sent since different system configurations may respond to different anomalous flag combinations differently.
What are next steps?	If the source of this event is an inside host, it is worth looking for other signs of recon activity. For example, is the host sending bad flag combinations to multiple hosts? Is it scanning many hosts on the same port? Is it scanning many ports on one host? An inside host performing reconnaissance can be a good sign of unwanted activity or compromise.
Non-standard flow data required? (FlowSensor, proxy, firewall,	For Flow Collector NetFlow edition, a FlowSensor is required. For Flow Collector sFlow, no special extras are required.

Questions about this event	Response
etc.)	
Notes	N/A

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	Enable Security event Bad_Flag_RST on the originating host.
Which policies have this event on by default?	Inside Hosts, Outside Hosts, Client IP Policy
Which policies have this event off by default?	Antivirus & SMS Servers; Firewalls, Proxies, & NAT Devices; Network Management & Scanners
Which policies have this alarm on by default?	None
Which policies have this alarm off by default?	Inside Hosts; Outside Hosts; Client IP Policy; Antivirus & SMS Servers; Firewalls, Proxies, & NAT Devices; Network Management & Scanners
Can you tune this event?	No
Is the event variance-based, threshold-based, or other?	N/A
What are default values and units?	
Tolerance	N/A
Minimum threshold value	N/A

Questions about event	Response
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	N/A
If so, what is it?	N/A

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host that sent the bad packet
What is the target?	The host listed as the bad packet's destination
Which policy causes the event to trigger?	The source's host policy
What alarm categories does this security event contribute to for the source?	High Recon Index, High Concern Index
In what quantity?	• High Recon Index: True

Questions about event	Response
	• CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: View details. Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source & target IP, a time range five minutes before the event's first active time until the event's last active time, the associated port as <port>/TCP and <port>/UDP, and TCP. Desktop Client: Flows are filtered by time period of last five minutes.

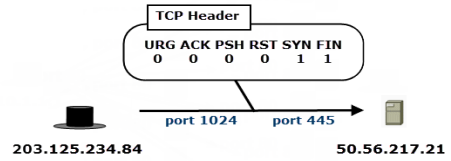
What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_BAD_FLAG_BAD_RST (266)

Bad Flag SYN (Synchronize) FIN (Finish) **

Mitigation is not available for the alarm associated with this security event.

Bad_Flag_SYN_FIN



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope Corporate	50.56.217.21	<CI value>*	Bad_Flag_SYN_FIN-445(1)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	If a packet is seen containing the TCP synchronize and finish flags, the security event is triggered on the originating host.
What does it mean when it triggers?	A TCP packet with invalid flags set should not normally happen. When it does happen, it has likely been done intentionally in an attempt to gather information about the machine to which the packet is sent since different system configurations may respond to different anomalous flag combinations differently.
What are next steps?	If the source of this event is an inside host, it is worth looking for other signs of recon activity. For example, is the host sending bad flag combinations to multiple hosts? Is it scanning many hosts on the same port? Is it scanning many ports on one host? An inside host performing reconnaissance can be a good sign of unwanted activity or compromise.
Non-standard flow data required? (FlowSensor, proxy, firewall,	For Flow Collector NetFlow edition, a FlowSensor is required. For Flow Collector sFlow, no special extras are required.

Questions about this event	Response
etc.)	
Notes	N/A

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	Enable Security event Bad_Flag_SYN_FIN on the originating host.
Which policies have this event on by default?	Inside Hosts, Outside Hosts, Client IP Policy
Which policies have this event off by default?	Antivirus & SMS Servers; Firewalls, Proxies, & NAT Devices; Network Management & Scanners
Which policies have this alarm on by default?	None
Which policies have this alarm off by default?	Inside Hosts; Outside Hosts; Client IP Policy; Antivirus & SMS Servers; Firewalls, Proxies, & NAT Devices; Network Management & Scanners
Can you tune this event?	No
Is the event variance-based, threshold-based, or other?	N/A
What are default values and units?	
Tolerance	N/A
Minimum threshold value	N/A

Questions about event	Response
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	N/A
If so, what is it?	N/A

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host that sent the bad packet
What is the target?	The host listed as the bad packet's destination
Which policy causes the event to trigger?	The source's host policy
What alarm categories does this security event contribute to for the source?	High Recon Index, High Concern Index
In what quantity?	• High Recon Index: True

Questions about event	Response
	• CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: View details. Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source & target IP, a time range five minutes before the event's first active time until the event's last active time, the associated port as <port>/TCP and <port>/UDP, and TCP. Desktop Client: Flows are filtered by time period of last five minutes.

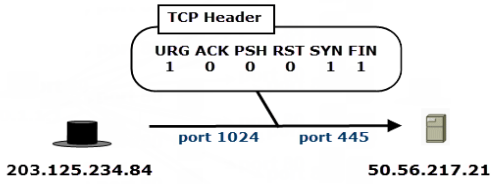
What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_BAD_FLAG_SYN_FIN (264)

Bad Flag URG (Urgent) **

Mitigation is not available for the alarm associated with this security event.

Bad_Flag_URG



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope Corporate	50.56.217.21	<CI value>*	Bad_Flag_URG-445(1)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	If a packet is seen containing the TCP urgent flag and any other flags besides acknowledge, the security event is triggered on the originating host.
What does it mean when it triggers?	A TCP packet with invalid flags set should not normally happen. When it does happen, it has likely been done intentionally in an attempt to gather information about the machine to which the packet is sent since different system configurations may respond to different anomalous flag combinations differently.
What are next steps?	If the source of this event is an inside host, it is worth looking for other signs of recon activity. For example, is the host sending bad flag combinations to multiple hosts? Is it scanning many hosts on the same port? Is it scanning many ports on one host? An inside host performing reconnaissance can be a good sign of unwanted activity or compromise.
Non-standard flow data required?	For Flow Collector NetFlow edition, a FlowSensor is required. For Flow Collector sFlow, no special extras

Questions about this event	Response
(FlowSensor, proxy, firewall, etc.)	are required.
Notes	N/A

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	Enable Security event Bad_Flag_URG on the originating host.
Which policies have this event on by default?	Inside Hosts, Outside Hosts, Client IP Policy
Which policies have this event off by default?	Antivirus & SMS Servers; Firewalls, Proxies, & NAT Devices; Network Management & Scanners
Which policies have this alarm on by default?	None
Which policies have this alarm off by default?	Inside Hosts; Outside Hosts; Client IP Policy; Antivirus & SMS Servers; Firewalls, Proxies, & NAT Devices; Network Management & Scanners
Can you tune this event?	No
Is the event variance-based, threshold-based, or other?	N/A
What are default values and units?	
Tolerance	N/A

Questions about event	Response
Minimum threshold value	N/A
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	N/A
If so, what is it?	N/A

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host that sent the bad packet
What is the target?	The host listed as the bad packet's destination
Which policy causes the event to trigger?	The source's host policy
What alarm categories does this security event contribute to for the source?	High Recon Index, High Concern Index

Questions about event	Response
In what quantity?	• High Recon Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: View details. Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source & target IP, a time range five minutes before the event's first active time until the event's last active time, the associated port as <port>/TCP and <port>/UDP, and TCP. Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_BAD_FLAG_URG (268)

Beaconing Host

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	An IP communication between an Inside Host and Outside Host (with traffic in only one direction) exceeds the "Seconds required to qualify a flow as long duration" setting.
What does it mean when it triggers?	A beaconing host is host looking for updates or commands from another. This traffic can be used for a variety of reasons, such as keep-alive (heartbeat), to obtain new orders from a Command and Control (C&C) server, or to download updates. It's important to realize that this behavior can be caused by malware, but that is not always the case.
What are next steps?	When investigating a Beaconing Host event, the goal is to determine if the Outside Host is indeed a C&C server. It can often be helpful to look this host up both inside of Secure Network Analytics and outside of it. A good first step within Secure Network Analytics is to open a Top Peers (Outbound) report on the target host. This will provide a list of inside peers sorted by the amount of data that have communicated with the Outside Host. This will tell you whether it is a very common peer within your environment or not. A second step would be to run a Flow Traffic report to visualize traffic patterns between the source and the Target. Communication with a C&C server will exhibit a periodic pattern with a fixed amount of outbound traffic.

Questions about this event	Response
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	None
Notes	This is the same as a unidirectional suspect long flow, but this event will trigger instead of a suspect long flow.

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	Enable security event Beaconing Host on the originating host.
Which policies have this event on by default?	Inside Hosts, Outside Hosts
Which policies have this event off by default?	none
Which policies have this alarm on by default?	none
Which policies have this alarm off by default?	Inside Hosts, Outside Hosts
Can you tune this event?	no
Is the event variance-based, threshold-based, or other?	N/A
What are default values and units?	N/A

Questions about event	Response
Tolerance	N/A
Minimum threshold value	N/A
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	
If so, what is it?	

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host that is beaconing
What is the target?	The host receiving the traffic from the beaconing Host
Which policy causes the event to trigger?	The source host policy
What alarm categories does this security event contribute	

Questions about event	Response
to for the source?	
In what quantity?	• High Command And Control Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	• TI: True

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: Source host W is using X Service Name (Y Protocol) as Peer to target Z. Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source & target IP, the start time (reset hour) of the event's active day until the event’s last active time, and client bytes & server bytes (both of which are greater than or equal to 0). Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_BEACONING_HOST (39)

Bot Command & Control Server

What is the security event?

Questions about this event	Response
What does it mean when it triggers?	Indicates that a host in your environment is being used to assist in the compromise of other hosts beyond your environment by acting as a command and control (C&C) server. This host is also very likely compromised itself.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	High Command And Control Index, High Concern Index
In what quantity?	• High Command And Control Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_COMMAND_AND_CONTROL_HOST (43)

Bot Infected Host - Attempted C&C Activity

What is the security event?

Questions about this event	Response
What does it mean when it triggers?	A host on your network has attempted to talk to a known command and control (C&C) server. Although the host was not successful in doing so, this is still concerning since something caused that host to make the attempt. Note that malware or a malicious redirect can also cause this behavior.
What are next steps?	This security event generally doesn't require too much validation within the product, but you should perform a flow query for flows between the target of the event and any other host to see if other hosts are interacting with the suspected C&C server. Set the time period of the query to the day of the event or longer. Depending on the duration of the communication, you can also use this query to determine when the source host began reaching out to the suspected C&C server. If you have many hosts communicating with the target host or you see historical communication, it is possible that the C&C server has been falsely identified.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	'Full' Policy: High Command And Control Index, High Concern Index 'Partial' Policy: High Command And Control Index, High Concern Index
In what quantity?	'Full' Policy: • High Command And Control Index: True • CI: True 'Partial' Policy: • High Command And Control Index: True • CI: True
What alarm categories does this security event contribute to for the target?	'Full' Policy: High Target Index 'Partial' Policy: High Target Index
In what quantity?	'Full' Policy: • TI: True 'Partial' Policy: • TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_BOT_INFECTED_HOST (41)

Bot Infected Host - Successful C&C Activity

What is the security event?

Questions about this event	Response
What does it mean when it triggers?	A host on your network has communicated with a known command and control (C&C) server. It is possible that this behavior has been caused by malware or a malicious redirect, or that this communication was an attempt at infection by, for example, an exploit kit. This is almost certainly sign of a compromised host.
What are next steps?	This security event generally doesn't require too much validation within the product, but you should perform a flow query for flows between the target of the event and any other host to see if other hosts are interacting with the suspected C&C server. Set the time period of the query to the day of the event or longer. Depending on the duration of the communication, you can also use this query to determine when the source host began reaching out to the suspected C&C server. If you have many hosts communicating with the target host or you see historical communication, it is possible that the C&C server has been falsely identified.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	'Full' Policy: High Command And Control Index, High Concern Index 'Partial' Policy: High Command And Control Index, High Concern Index
In what quantity?	'Full' Policy: • High Command And Control Index: True • CI: True 'Partial' Policy: • High Command And Control Index: True • CI: True
What alarm categories does this security event contribute to for the target?	'Full' Policy: High Target Index 'Partial' Policy: High Target Index
In what quantity?	'Full' Policy: • TI: True 'Partial' Policy: • TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_BOT_INFECTED_HOST_CONTROLLED (42)

Brute Force Login

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	The host detects a series of short TCP connections consistent with an attempt at brute force password cracking through repeated logins.
What does it mean when it triggers?	This may be indicative of a host trying to guess login credentials against another in an attempt to gain access to the system. It may also indicate a misconfigured application on the client which is attempting numerous repeat connections to the server and failing authentication.
What are next steps?	The goal is to determine if the connection attempt to the server is legitimate. If the client is an outside host, is the client address part of a known trusted or business partner network that may be expected to initiate these connections? If so, it may be a misconfigured application. You should also run an external lookup against DShield (for the target host) to verify the owner of the target IP in the security event alarm. If the client is an inside host, would this host be expected to attempt these types of connections to the server in question? Running a Top Peers report for the source host may tell you if this host is connecting to other hosts on the network with similar byte counts or high number of flows. You can also run a Top Ports report to find other hosts that the source IP is connecting to over the same port for which the security event alarm triggered (probably SSH).
Non-standard flow data required? (FlowSensor, proxy, firewall,	none

Questions about this event	Response
etc.)	
Notes	None

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	
Which policies have this event on by default?	Inside Hosts, Outside Hosts
Which policies have this event off by default?	
Which policies have this alarm on by default?	
Which policies have this alarm off by default?	Inside Hosts, Outside Hosts
Can you tune this event?	Yes
Is the event variance-based, threshold-based, or other?	N/A
What are default values and units?	N/A
Tolerance	N/A
Minimum threshold value	1 (number of connections) and 1 (average bytes per connection)

Questions about event	Response
Maximum threshold value	3,000 (number of connections) and 50,000 (average bytes per connection)
Is event tunable with non-variance-based parameters?	Number of connections and average bytes per connection.
If so, what are its tunable attributes and units?	N/A
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	
If so, what is it?	

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The attacking host
What is the target?	The victim host
Which policy causes the event to trigger?	
What alarm categories does this security event contribute to for the source?	
In what quantity?	• Attack Index: True

Questions about event	Response
	• CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	• TI: True

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: View details. Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source & target IP, the start time (reset hour) of the event's active day until the event's last active time, and the associated port as <port>/TCP. Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_BRUTE_FORCE_LOGIN (58)

Connection from Bogon Address Attempted

What is the security event?

Questions about this event	Response
What does it mean when it triggers?	A bogon address is an IP address which has not been assigned and should not be used. Unidirectional communication from one is generally not very concerning, however, it should not happen during regular use. In fact, this sort of traffic is often blocked at a network's perimeter. A specific type of behavior to look for when seen in bulk is a denial-of-service (DoS) attack in which an attacker is spoofing source IP addresses.
What are next steps?	There are two things to initially look for when investigating unidirectional traffic from a bogon address: 1) Is the bogon address (or other bogon addresses) attempting to communicate with other hosts in your network? 2) Is the host to which traffic is being sent from a bogon address receiving an abnormally large amount of traffic? To answer the first question, you can run either a Top Hosts query or a flow query against the bogon host group. You can run it specifically against the bogon IP from the security event, but in the event of spoofed traffic it is trivial for an attacker to use many different bogon IPs. Assess the results returned from your query to determine whether or not this is part of a DoS attack or is potentially a misconfiguration / unclassified host in your network. Generally, a large volume of data or packets is a sign of a DoS attack. To answer the second question, focus your query on the target host of the security event, since the goal is to find out if there is an abnormally large amount of traffic, whether from that bogon address or not. A quick way

Questions about this event	Response
	to get some helpful information is to view the target host's other security events and look for DoS events like SYNs Received or New Flows Served, or look for an abundance of communication from bogons. To investigate a bit more thoroughly, run a Flow Traffic report. Set the Date/Time filter to include the time of the bogon communication as well as two hours before this. A longer time window will result in a longer query but will provide you with better context. Here you can also filter the hosts to include traffic only from outside hosts if you are not concerned about an internally launched DoS attack. A large spike or even a gradual but large volume of traffic may be indicative of a DoS attack.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	High Concern Index
In what quantity?	• CI: True
What alarm categories does this security event contribute	Anomaly Index, High Ddos Target Index, High Target Index

Questions about event	Response
to for the target?	
In what quantity?	• Anomaly Index: True • High Ddos Target Index: True • TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_CONN_FROM_BOGON_ATTEMPTED (519)

Connection from Bogon Address Successful

What is the security event?

Questions about this event	Response
What does it mean when it triggers?	A bogon address is an IP address which has not been assigned and should not be used. Bidirectional communication with a bogon address should not occur. This behavior is most likely a sign of a misconfiguration within either your network or your Secure Network Analytics deployment.
What are next steps?	Determine if your environment actually uses a particular bogon IP address range internally or whether or not you use Carrier Grade NAT. If your environment uses a bogon range internally and that is expected, simply add the range to your Inside Hosts group. A way to check this within Secure Network Analytics is to look for active flows in the /24 of the bogon. If a large part of the range is active, it is likely a range being purposefully used within your environment. If the bogon IP is within 100.64.0.0/10, it is using IP space reserved for Carrier Grade NAT and is not an issue if your environment is behind one. If neither of these is the case, the Host Snapshot (accessed within the Desktop Client) will contain information to help you identify the host. For example, the Exporter Interface tab displays which exporters and interfaces are seeing the host's flows to help you determine where the device is hosted. In addition, check out the Security Events tab, Alarms tab, and Identification tabs. These will show you any other behavior with which the bogon host has been involved. Finally, view the security events of the bogon host to see if there are any other hosts it has interacted with.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	High Concern Index
In what quantity?	• CI: True
What alarm categories does this security event contribute to for the target?	Anomaly Index, High Ddos Target Index, High Target Index
In what quantity?	• Anomaly Index: True • High Ddos Target Index: True • TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_CONN_FROM_BOGON_SUCCEEDED (517)

Connection from Tor Attempted

Detects attempted connections to host(s) inside your network from Tor exit nodes.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	High Policy Violation Index, High Concern Index
In what quantity?	• High Policy Violation Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_TOR_EXIT_ATTEMPTED (317)

Connection from Tor Successful

Detects successful connections to host(s) inside your network from Tor exit nodes.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	High Policy Violation Index, High Concern Index
In what quantity?	• High Policy Violation Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_TOR_EXIT_SUCCEEDED (318)

Connection to Bogon Address Attempted

What is the security event?

Questions about this event	Response
What does it mean when it triggers?	A bogon address is an IP address which has not been assigned and should not be used. Unidirectional communication to one is a bit peculiar, since something must have prompted a host in your network to do so. It is possible that this is backscatter from a denial-of-service (DoS) attack. This occurs when an attacker sends you packets with randomized source address as part of a distributed denial-of-service (DDoS) and you respond to those randomized addresses. If an attacker is randomizing the entire IP space, some of these will be bogon addresses. Unidirectional communication to a bogon IP may also be a sign of reconnaissance or a misconfigured host.
What are next steps?	Determine if your environment actually uses a particular bogon IP address range internally or whether or not you use Carrier Grade NAT. If your environment uses a bogon range internally and that is expected, simply add the range to your Inside Hosts group. A way to check this within Secure Network Analytics is to look for active flows in the /24 of the bogon. If a large part of the range is active, it is likely a range being purposefully used within your environment. If the bogon IP is within 100.64.0.0/10, it is using IP space reserved for Carrier Grade NAT and is not an issue if your environment is behind one. If neither of these are the case, review the other security events on the source of the event. Look for either an abundance of communication to bogons or denial-of-service (DoS) events like SYNs Received or New Flows Served. Also, look for recon-related events

Questions about this event	Response
	such as Ping Scan or Addr_Scan. To investigate a potential DDoS bit more thoroughly, run a Flow Traffic report. Set the Date/Time filter to include the time of the Bogon communication as well as two hours before this. A longer time window will result in a longer query but will provide you with better context. Here you can also filter the hosts to include traffic only from outside hosts if you are not concerned about an internally launched DoS attack. A large spike or even a gradual but large volume of traffic may be indicative of a DoS attack. If neither a DDoS or a large number of reconnaissance activity seem likely, view the security events of the bogon IP to see if there are any other hosts that have attempted to interact with the bogon host. A large number of hosts attempting to interact with a particular bogon suggest either an application had a bad configuration pushed out or an application hosted on a bogon range disappeared. You can investigate this further by viewing the bogon's historical traffic.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute	Anomaly Index, High Concern Index

Questions about event	Response
to for the source?	
In what quantity?	• Anomaly Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_CONN_TO_BOGON_ATTEMPTED (518)

Connection to Bogon Address Successful

What is the security event?

Questions about this event	Response
What does it mean when it triggers?	A bogon address is an IP address which has not been assigned and should not be used. Bidirectional communication with a bogon address should not occur. This behavior is most likely a sign of a misconfiguration within either your network or your Secure Network Analytics deployment.
What are next steps?	Determine if your environment actually uses a particular bogon IP address range internally or whether or not you use Carrier Grade NAT. If your environment uses a bogon range internally and that is expected, simply add the range to your Inside Hosts group. A way to check this within Secure Network Analytics is to look for active flows in the /24 of the bogon. If a large part of the range is active, it is likely a range being purposefully used within your environment. If the bogon IP is within 100.64.0.0/10, it is using IP space reserved for Carrier Grade NAT and is not an issue if your environment is behind one. If neither of these is the case, the Host Snapshot (accessed within the Desktop Client) will contain information to help you identify the host. For example, the Exporter Interface tab displays which exporters and interfaces are seeing the host's flows to help you determine where the device is hosted. In addition, check out the Security Events tab, Alarms tab, and Identification tabs. These will show you any other behavior with which the bogon host has been involved. Finally, view the security events of the bogon host to see if there are any other hosts it has interacted with.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	Anomaly Index, High Concern Index
In what quantity?	• Anomaly Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_CONN_TO_BOGON_SUCCEEDED (516)

Connection to Tor Attempted

What is the security event?

Questions about this event	Response
What does it mean when it triggers?	Tor, formerly The Onion Router, is a network used for anonymizing Internet connections which works by sending a connection through multiple relays before exiting the Tor network. A Tor entry node is the first server a Tor connection transits through before navigating and exiting the Tor network. This security event involves a host that is being monitored by Secure Network Analytics attempting to communicate with a Tor entry node but that was not observed establishing a successful connection. It is possible that this was either user-driven or malware attempting to find command and control traffic. If it was user-driven, this was likely an attempt at obfuscating the destination of the user's traffic or obfuscating the location from where the user was browsing. It is important to note that some Tor entry nodes run on servers that also run other services. For example, DuckDuckGo runs Tor entry nodes on the same server that is accessed to perform searches.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	High Policy Violation Index, High Concern Index
In what quantity?	• High Policy Violation Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_TOR_ENTRY_ATTEMPTED (513)

Connection to Tor Successful

What is the security event?

Questions about this event	Response
What does it mean when it triggers?	Tor, formerly The Onion Router, is a network used for anonymizing Internet connections which works by sending a connection through multiple relays before exiting the Tor network. A Tor entry node is the first server a Tor connection transits through before navigating and exiting the Tor network. This security event involves a host that is being monitored by Secure Network Analytics communicating with a Tor entry node. It is possible that this as either user-driven or malware attempting to find command and control traffic. If it was user-driven, this was likely an attempt at obfuscating the destination of the user's traffic or obfuscating the location from where the user was browsing. It is important to note that some Tor entry nodes run on servers that also run other services. For example, DuckDuckGo runs Tor entry nodes on the same server that is accessed to perform searches.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	High Policy Violation Index, High Concern Index
In what quantity?	• High Policy Violation Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_TOR_ENTRY_SUCCEEDED (514)

Fake Application Detected

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	When processing updates to the application list for a host, a method is called to determine if the application data being processed is a fake application. The fake app logic takes the data from the current flow being analyzed along with the information for the hosts involved. Using this data the algorithm determines if the protocol (TCP or UDP) and ports being used match the expected application identified. The application identification comes from one of the following devices depending on how the network is configured (FlowSensor, Palo Alto Appliance, Packetshaper Appliance, or NBar Appliance). Currently monitored applications include telnet, SSH FTP, mail services, NTP, and DNS. The alarm will trigger if a standard application uses a non-standard port (For example, DNS over 123/udp), or if a particular port has a non-standard application communicating over it (For example, SSH over 80/tcp).
What does it mean when it triggers?	This behavior is often a sign of a person or application attempting to circumvent egress filtering by sending traffic out of a commonly permitted port using a service other than the one intended. It will also look for standard applications over ports other than their standard which can cause it to occasionally fire on applications using secondary ports, like SSH over TCP 8022.
What are next steps?	The goal of your investigation is to find the relevant flows, and then to attempt to determine whether or not they appear to be signs of exfiltration or command and control.

Questions about this event	Response
	A first step in investigating this event is to consider the port attached to the event and the hosts involved. For example, if the target host is an offsite backup server and the event triggered on port 8022 that may not be of concern. On the other hand, if the target host is unfamiliar and you see non-DNS going out over 53 UDP it's likely worth a deeper look. There are a few options to investigate this- the event will list an associated port, and you can use it to build a very specific filter. For example, if you filter for flows between the two involved hosts over the involved port but also exclude flows using the 'proper' application (e.g. searching for flows over port 53 UDP that are not DNS) you'll find the flows that caused the event to fire. It may also be useful to run a more general query instead, filtering on just the source and target host of the event on the date of the event. This may turn up flows beyond just any that have a port / application mismatch, but the existence of any such flows may actual be valuable context in an investigation. Once you have a selection of flows to work with, examine the destination host, history, and data volume for signs of misuse.
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	Requires additional information from a FlowSensor, Palo Alto Appliance, Packetshaper Appliance, or NBar Appliance.
Notes	None.

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	
Which policies have this event on by default?	Inside Hosts, Outside Hosts
Which policies have this event off by default?	
Which policies have this alarm on by default?	
Which policies have this alarm off by default?	Inside Hosts, Outside Hosts
Can you tune this event?	no
Is the event variance-based, threshold-based, or other?	N/A
What are default values and units?	N/A
Tolerance	N/A
Minimum threshold value	N/A
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A

Questions about event	Response
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	
If so, what is it?	

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	N/A
What is the target?	N/A
Which policy causes the event to trigger?	N/A
What alarm categories does this security event contribute to for the source?	High Command And Control Index, High Concern Index
In what quantity?	• High Command And Control Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: A host has used X over Port/Protocol (ServiceName). Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source & target IP, a time range 35 minutes before the event's first active time until the event's last active time, and the associated port as <port>/TCP and <port>/UDP. Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_FAKE_APP (62)

Flow Denied

Mitigation is not available for the alarm associated with this security event.

What is the security event?

Questions about this event	Response
What does it mean when it triggers?	This is largely dependent on context. For example, Flow Denied from a host on the Internet is likely not that interesting, especially as a single event. Flow Denied from an inside host to an inside host is different from inside to outside, and trying the same host/port pairing over and over again is much different from getting blocked to a variety of destinations. If an inside host has many denied flows talking to another inside host over one port, it is likely a misconfiguration. Many denied flows to a variety of ports or inside hosts is likely reconnaissance. Apart from that, it is a sign of a host doing things that you have determined it should not do, which makes it inherently interesting. Flows blocked from an inside host to the Internet require the context of what rules it is attempting to violate, but regardless, the host is doing something that your security policy has determined it should not be able to do.
What are next steps?	A good way to investigate Flows Denied is to perform a security event query on the source host of the event. Run the query for the day of the event, set the source host to be the source of the initial Flow Denied event, and then set the type to include only other Flow Denied events. This will show you all of the Flow Denied events for the host. From the returned results you can determine whether it was a single denied flow, many denied flows over the same port to the same host, many denied flows to different hosts over the same port, many denied flows to the same host group, etc.

Questions about this event	Response
	This will enable you to figure out what behavior the host is actually engaging in.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	High Recon Index, High Concern Index
In what quantity?	• High Recon Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

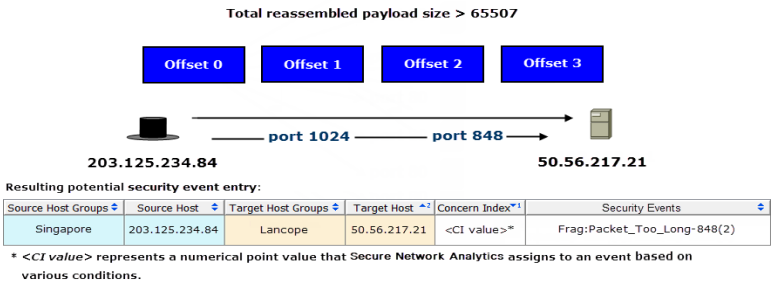
What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_FLOW_DENIED (310)

Frag Packet Too Long **

Mitigation is not available for the alarm associated with this security event.

Frag:Packet_Too_Long



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope	50.56.217.21	<CI value>*	Frag:Packet_Too_Long-848(2)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	If a packet is seen with fragmentation values that would cause the packet to exceed the maximum packet length, the security event triggers on the originating host.
What does it mean when it triggers?	An IP packet with an invalid fragmentation value is not something that should normally happen. When it happens it has likely been done intentionally in an attempt to gather information about the machine the packet is sent to as different operating systems and versions may respond differently.
What are next steps?	If the source of this event is an inside host, it is worth looking for other signs of recon activity. For example, is the host sending invalid fragments to multiple hosts? Is it scanning many hosts on the same port? Is it scanning many ports on one host? An inside host performing reconnaissance can be a good sign of unwanted activity or compromise.
Non-standard flow data required?	For Flow Collector NetFlow edition, a FlowSensor is required. For Flow Collector sFlow, no special extras

Questions about this event	Response
(FlowSensor, proxy, firewall, etc.)	are required.
Notes	N/A

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	Security event Frag:Packet_Too_Long must be enabled on the originating host
Which policies have this event on by default?	Inside Hosts, Outside Hosts, Client IP Policy
Which policies have this event off by default?	Antivirus & SMS Servers; Firewalls, Proxies, & NAT Devices; Network Management & Scanners
Which policies have this alarm on by default?	None
Which policies have this alarm off by default?	Inside Hosts; Outside Hosts; Client IP Policy; Antivirus & SMS Servers; Firewalls, Proxies, & NAT Devices; Network Management & Scanners
Can you tune this event?	No
Is the event variance-based, threshold-based, or other?	N/A
What are default values and units?	
Tolerance	N/A

Questions about event	Response
Minimum threshold value	N/A
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	N/A
If so, what is it?	N/A

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host that sent the bad packet
What is the target?	The host listed as the bad packet's destination
Which policy causes the event to trigger?	Source host policy
What alarm categories does this security event contribute to for the source?	Attack Index, High Concern Index

Questions about event	Response
In what quantity?	• Attack Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available in Secure Network Analytics?

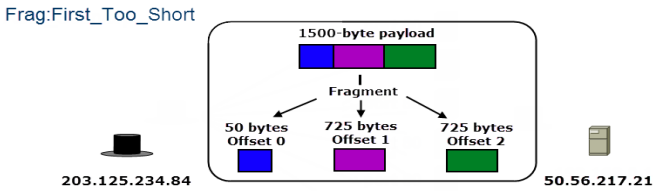
Questions about event	Response
What information is displayed in the alarm details?	Manager: View details. Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source & target IP, a time range one minute before the event's first active time until the event's last active time, and TCP. Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_FRAG_PKT_TOO_LONG (282)

Frag Packet Too Short **

Mitigation is not available for the alarm associated with this security event.



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope	50.56.217.21	<CI value>*	Frag:First_Too_Short-445(1)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	If a packet is seen with a fragmentation length so short that the protocol headers are truncated, the security event triggers on the originating host.
What does it mean when it triggers?	An IP packet with an invalid fragmentation value is not something that should normally happen. When it happens it has likely been done intentionally in an attempt to gather information about the machine the packet is sent to as different operating systems and versions may respond differently.
What are next steps?	If the source of this event is an inside host, it is worth looking for other signs of recon activity. For example, is the host sending invalid fragments to multiple hosts? Is it scanning many hosts on the same port? Is it scanning many ports on one host? An inside host performing reconnaissance can be a good sign of unwanted activity or compromise.
Non-standard flow data required? (FlowSensor, proxy, firewall,	For Flow Collector NetFlow edition, a FlowSensor is required. For Flow Collector sFlow, no special extras are required.

Questions about this event	Response
etc.)	
Notes	N/A

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	Security event Frag:First_Too_Short must be enabled on the originating host
Which policies have this event on by default?	Inside Hosts, Outside Hosts, Client IP Policy
Which policies have this event off by default?	Antivirus & SMS Servers; Firewalls, Proxies, & NAT Devices; Network Management & Scanners
Which policies have this alarm on by default?	None
Which policies have this alarm off by default?	Inside Hosts; Outside Hosts; Client IP Policy; Antivirus & SMS Servers; Firewalls, Proxies, & NAT Devices; Network Management & Scanners
Can you tune this event?	No
Is the event variance-based, threshold-based, or other?	N/A
What are default values and units?	
Tolerance	N/A
Minimum threshold value	N/A

Questions about event	Response
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	N/A
If so, what is it?	N/A

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host that sent the bad packet
What is the target?	The host listed as the bad packet's destination
Which policy causes the event to trigger?	Source host policy
What alarm categories does this security event contribute to for the source?	Attack Index, High Concern Index
In what quantity?	• Attack Index: True

Questions about event	Response
	• CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: View details. Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source & target IP, a time range one minute before the event's first active time until the event's last active time, and TCP. Desktop Client: Flows are filtered by time period of last five minutes.

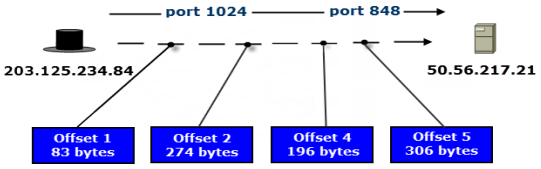
What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_FRAG_PKT_TOO_SHORT (281)

Frag Sizes Differ **

Mitigation is not available for the alarm associated with this security event.

Frag:Sizes_Differ



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope	50.56.217.21	<CI value>*	Frag:Sizes_Differ-848(2)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	If a packet is seen with fragmentation sizes that differ between segments, the security event triggers on the originating host.
What does it mean when it triggers?	An IP packet with different fragmentation sizes for each segment is not something that should normally happen. When it happens it has likely been done intentionally in an attempt to evade packet inspection tools along its route.
What are next steps?	If the source of this event is an inside host, it is worth looking for other signs of recon activity. For example, is the host sending invalid fragments to multiple hosts? Is it scanning many hosts on the same port? Is it scanning many ports on one host? An inside host performing reconnaissance can be a good sign of unwanted activity or compromise.
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	For Flow Collector NetFlow edition, a FlowSensor is required. For Flow Collector sFlow, no special extras are required.

Questions about this event	Response
Notes	N/A

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	Security event Frag:Sizes_Differ must be enabled on the originating host.
Which policies have this event on by default?	Inside Hosts, Outside Hosts, Client IP Policy
Which policies have this event off by default?	Antivirus & SMS Servers; Firewalls, Proxies, & NAT Devices; Network Management & Scanners
Which policies have this alarm on by default?	None
Which policies have this alarm off by default?	Inside Hosts; Outside Hosts; Client IP Policy; Antivirus & SMS Servers; Firewalls, Proxies, & NAT Devices; Network Management & Scanners
Can you tune this event?	No
Is the event variance-based, threshold-based, or other?	N/A
What are default values and units?	
Tolerance	N/A
Minimum threshold value	N/A
Maximum threshold value	N/A

Questions about event	Response
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	N/A
If so, what is it?	N/A

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host that sent the bad packet
What is the target?	The host listed as the bad packet's destination
Which policy causes the event to trigger?	Source host policy
What alarm categories does this security event contribute to for the source?	Attack Index, High Concern Index
In what quantity?	• Attack Index: True • CI: True

Questions about event	Response
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available in Secure Network Analytics?

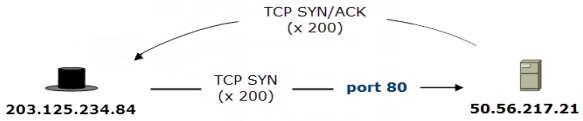
Questions about event	Response
What information is displayed in the alarm details?	Manager: View details. Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source & target IP, a time range one minute before the event's first active time until the event's last active time, and TCP. Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_FRAG_DIFFERENT_SIZES (283)

Half Open Attack

Half_Open_Attack



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope	50.56.217.21	<CI value>*	Half_Open_Attack

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

What is the security event?

Questions about this event	Response
What does it mean when it triggers?	This is a denial-of-service (DoS) attack. It is possible that a half open attack can be an attempt to exhaust either bandwidth or connection handlers since it opens connections but never carries them out, forcing the victim host to wait long enough to cause the malicious connections to time out.
What are next steps?	The goal is to determine if the connections to the target are legitimate and if the target experiences any performance degradation. While it is possible that this can be malicious behavior between two inside hosts, the event is more likely to be interesting between an inside and outside host. First, run a flow query between the source and target of the event for the day of the event. Take note of whether the flow is ongoing. If it is not, and there was no service outage, it was likely not an issue. You can also check the security event history of both the source and target hosts. Does the source host have this event against multiple targets or historically? If so, this is something to research further. Does the target host have many hosts triggering this

Questions about this event	Response
	event against it at once but not historically? This may be sign of a distributed denial-of-servce (DDoS) attack. If the event is also firing historically, it may just be normal behavior for whatever application the service is hosting. If this is the case, consider turning t he event off for the particular host. If the relevant traffic was observed by a Flow Sensor, run a performance report to see if the SRT (Server Response Time) has been affected due to the nature of the traffic. This could indicate whether or not this is legitimate traffic.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	'A' Policy: High Ddos Source Index, High Concern Index 'B' Policy: High Ddos Source Index, High Concern Index
In what quantity?	'A' Policy: • High Ddos Source Index: True • CI: True 'B' Policy:

Questions about event	Response
	• High Ddos Source Index: True • CI: True
What alarm categories does this security event contribute to for the target?	'A' Policy: High Ddos Target Index, High Target Index 'B' Policy: High Ddos Target Index, High Target Index
In what quantity?	'A' Policy: • High Ddos Target Index: True • TI: True 'B' Policy: • High Ddos Target Index: True • TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_HALF_OPEN (26)

High File Sharing Index

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	It searches for large data transfers that do not originate from a file server. The source (the host downloading the large amount of data) may be using peer-to-peer techniques or simple file sharing methods and protocols to download large files from the target.
What does it mean when it triggers?	The source is likely downloading an unusual amount of data from the target. This is a potential precursor to Data Hoarding and Data Exfiltration.
What are next steps?	Determine how much data was downloaded. As this may be a precursor to Suspect Data Hoarding, the steps are the same, except the initial target is known in this case. An ideal way to investigate this is to run a Top Peers (inbound) report for the source. Set the time period of the query to be the day of the event. Filter the report so that *Client* or *Server Host* is the source IP of the security event and *Other Host* is the Inside Hosts' host group. The goal is to find whether or not the source has done this across many targets. If the target is the only host sending data to the source, run a Top Peers report for the target to see if it has exhibited the same activity with other hosts. If so, it is worth investigating the target as the file sharing server to see if the activity is expected.
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	none
Notes	N/A

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	
Which policies have this event on by default?	Inside Host
Which policies have this event off by default?	Outside Host
Which policies have this alarm on by default?	Inside Host on by defualt
Which policies have this alarm off by default?	Outside Host
Can you tune this event?	yes
Is the event variance-based, threshold-based, or other?	variance
What are default values and units?	N/A
Tolerance	75
Minimum threshold value	100,000 FSI points in 24 hours
Maximum threshold value	1,000,000,000 FSI points in 24 hours
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A

Questions about event	Response
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	
If so, what is it?	

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host that is receiving the files.
What is the target?	The hosts that are sending the files.
Which policy causes the event to trigger?	
What alarm categories does this security event contribute to for the source?	
In what quantity?	• High Policy Violation Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: Observed W points. Expected X points, tolerance of Y allows up to Z points. Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source IP and Outside Hosts and the start time (reset hour) of the event's active day until the event’s last active time. Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_FILE_SHARING (20)

High SMB Peers

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	The host has many Server Message Block (SMB) sessions to the outside, which is consistent with worm propagation.
What does it mean when it triggers?	Unless you know that this should be happening in a particular scenario, or you have set the threshold very low, this event is almost certainly a sign of a compromised host. It is often a sign of malware looking to spread automatically via SMB.
What are next steps?	This security event is a probable sign of compromise, but you can investigate it to see if the outside hosts belong to a particular range or to see how many of them have been contacted. To do this, start a flow query. Set the start time of the query to the day of the event. On the Filter dialog, on the Hosts tab, set Client or Server Host as the source of the event and Other Host is the Inside Hosts host group. On the Services & Applications tab, filter by Services and include SMB. The query returns all relevant flows.
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	None
Notes	None

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	
Which policies have this event on by default?	Inside Host, Outside Host
Which policies have this event off by default?	
Which policies have this alarm on by default?	
Which policies have this alarm off by default?	Inside Host, Outside Host
Can you tune this event?	Yes
Is the event variance-based, threshold-based, or other?	Threshold
What are default values and units?	
Tolerance	N/A
Minimum threshold value	100 SMB flows from an Inside Host to an Outside Host.
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A

Questions about event	Response
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	
If so, what is it?	

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The Inside Host with many Manager peers
What is the target?	The hosts that are acting as SMB peers.
Which policy causes the event to trigger?	
What alarm categories does this security event contribute to for the source?	
In what quantity?	• High Recon Index: True • Attack Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	• TI: True

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: View details. Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source IP & Outside Hosts, the start time (reset hour) of the event's active day until the event’s last active time, 445/TCP, and 445/UDP. Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_HIGH_SMB_PEERS (60)

High Total Traffic

What is the security event?

Questions about this event	Response
What does it mean when it triggers?	Due to counting both inbound and outbound traffic, High Total Traffic is a general sign of anomalous behavior. It may be predominantly inbound, predominantly outbound, or a mixture of the two. The IP is simply involved in an abnormally higher amount of traffic.
What are next steps?	Determine how much data is moving and where that data is going to and coming from. An ideal way to investigate this is to perform a flow query for the source host. Set the time period to the day of the associated security event, and set the source host to be the client host or server host. Once the results have returned, find where the highest volume of data was going to or coming from; sort by Total Bytes to do this. The goal is to find the standout flow(s). After finding the standout flow(s), determine whether or not this is expected behavior.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	Anomaly Index, High Concern Index
In what quantity?	• Anomaly Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_TOTAL_TRAFFIC (16)

High Traffic

What is the security event?

Questions about this event	Response
What does it mean when it triggers?	Due to counting both inbound and outbound traffic, High Traffic is a general sign of anomalous behavior. It may be predominantly inbound, predominantly outbound, or a mixture of the two. The IP is simply involved in an abnormally higher amount of traffic. It is a possible indicator of incoming or outgoing DoS.
What are next steps?	Determine how much data is moving and where that data is going to and coming from. An ideal way to investigate this is to perform a flow query for the source host. Set the start time of the query to five minutes before the start time of the associated security event, and set the end time to the end time of the alarm (if there is an alarm). Set the source host to be the client host or server host. Once the results have returned, find where the highest volume of data was going to or coming from; sort by Total Bytes to do this. The goal is to find the standout flow(s). After finding the standout flow(s), determine whether or not this is expected behavior.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	Anomaly Index, High Concern Index
In what quantity?	• Anomaly Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_HI_TRAFFIC (30)

High Volume Email

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	It searches for hosts that have not been specified as Email servers but are displaying very large outgoing email bursts in relation to a small or non-existent incoming email ratio.
What does it mean when it triggers?	The host alerted on is potentially infected with a piece of email worm malware, or the host has been re-purposed for spamming.
What are next steps?	Determine the amount of data per flow going out and over which ports it is sending them out. Run two Top Peer reports—one filtered by protocol and one filtered by flows—to see whether the host is propagating a worm across the network or is being used as an SMTP relay for spam purposes. Determine whether or not data being sent from these peers in the observed quantity is expected behavior.
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	FlowSensor is required for acquiring and working with NetFlow
Notes	N/A

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event	

Questions about event	Response
to trigger?	
Which policies have this event on by default?	Inside Hosts, Outside Hosts
Which policies have this event off by default?	
Which policies have this alarm on by default?	Inside Hosts, Outside Hosts
Which policies have this alarm off by default?	
Can you tune this event?	yes
Is the event variance-based, threshold-based, or other?	Threshold
What are default values and units?	N/A
Tolerance	N/A
Minimum threshold value	N/A
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	Five-minute periods with High Volume Email Alerts to trigger the alarm; defaults to 1.
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate	N/A

Questions about event	Response
locations of tunable values?	
Does event have a default mitigation?	
If so, what is it?	

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host that is being scanned
What is the target?	No target host.
Which policy causes the event to trigger?	
What alarm categories does this security event contribute to for the source?	
In what quantity?	• High Policy Violation Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: View details Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source IP, the start time (reset hour) of the event's active day until the event's last active time, and 25/TCP. Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_HIGH_VOLUME_EMAIL (9)

ICMP Comm (Communication) Admin **

The source host has received an ICMP message that "communication is administratively prohibited." This is generated if a router cannot forward a packet due to administrative filtering.

Mitigation is not available for the alarm associated with this security event.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	High Recon Index, High Concern Index
In what quantity?	• High Recon Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_COMM_ADMIN_PROHIBITED (302)

ICMP Dest (Destination) Host Admin **

The source host has received an ICMP message stating that the "destination host is administratively prohibited."

Mitigation is not available for the alarm associated with this security event.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	High Recon Index, High Concern Index
In what quantity?	• High Recon Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_DEST_HOST_ADMIN_PROHIBITED (299)

ICMP Dest (Destination) Host Unk (Unknown)**

The source host has received an ICMP message that a "destination host unknown" error has occurred.

Mitigation is not available for the alarm associated with this security event.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	High Recon Index, High Concern Index
In what quantity?	• High Recon Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_DEST_HOST_UNKNOWN (296)

ICMP Dest (Destination) Net Admin **

The source host has received an ICMP message that the "destination network is administratively prohibited."

Mitigation is not available for the alarm associated with this security event.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	High Recon Index, High Concern Index
In what quantity?	• High Recon Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_DEST_NETWK_ADMIN_PROHIBITED (298)

ICMP Dest (Destination) Net Unk (Unknown) **

The source host has received an ICMP message that a "destination network unknown" error has occurred.

Mitigation is not available for the alarm associated with this security event.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	High Recon Index, High Concern Index
In what quantity?	• High Recon Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_DEST_NETWORK_UNKNOWN (295)

ICMP Flood

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	The source host has sent an excessive number of ICMP packets in a 5-minute period.
What does it mean when it triggers?	This indicates that the source host is engaged in a DoS attack (potentially caused by either a compromised host or driven by a user), a misconfigured network application, or a reconnaissance (during which the packets are sent across a very wide range of IPs rather than across a small group).
What are next steps?	Determine how many ICMP packets are being sent at what rate, when they were sent, and where they are going. An ideal way to investigate this is to perform a flow query for the source host. Set the start time of the query to five minutes before the start time of the associated security event, and set the end time to the end time of the alarm (if there is an alarm). Set the protocol filter to ICMP only. Once the results have returned, find where the most ICMP packets went during the searched time period. If the subject of the event is the client host in its ICMP- heavy flows, you can sort on Client Packets or Client Packet Rate (pps). The goal is to find the standout flow(s). After finding the standout flow(s), determine whether or not this is expected behavior.
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	None
Notes	N/A

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	
Which policies have this event on by default?	Inside Hosts, Outside Hosts
Which policies have this event off by default?	
Which policies have this alarm on by default?	Inside Hosts, Outside Hosts
Which policies have this alarm off by default?	
Can you tune this event?	Yes
Is the event variance-based, threshold-based, or other?	Behavioral and Threshold
What are default values and units?	
Tolerance	75
Minimum threshold value	1,800 ICMP Packets in 5 minutes
Maximum threshold value	10 Million ICMP Packets in 5 minutes
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A

Questions about event	Response
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	
If so, what is it?	

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host receiving the ICMP Packets
What is the target?	N/A
Which policy causes the event to trigger?	
What alarm categories does this security event contribute to for the source?	
In what quantity?	• High Ddos Source Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: Observed X pp5m. Expected Y pp5m, tolerance of Z allows up to Y pp5m. Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source IP, a time range five minutes before the event's first active time until the event's last active time, and ICMP. Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_ICMP_FLOOD (7)

ICMP Frag (Fragmentation) Needed **

The source host has received an ICMP message stating that "the IP datagram is too big". Packet fragmentation is required, but the DF bit in the IP header is set.

Mitigation is not available for the alarm associated with this security event.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	Anomaly Index, High Concern Index
In what quantity?	• Anomaly Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_FRAG_NEEDED_DF_SET (293)

ICMP Host Precedence **

The source host has received an ICMP message that "host precedence violation" has occurred. Sent by the first hop router to a host to indicate that a requested precedence is not permitted for the particular combination of source/destination host or network, upper layer protocol, and source/destination port.

Mitigation is not available for the alarm associated with this security event.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	Anomaly Index, High Concern Index
In what quantity?	• Anomaly Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_HOST_PRECEDENCE_VIOLATION (303)

ICMP Host Unreach **

The source host has received an ICMP message that the "target host is unreachable."

Mitigation is not available for the alarm associated with this security event.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	High Recon Index, High Concern Index
In what quantity?	• High Recon Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_HOST_UNREACHABLE (290)

ICMP Host Unreach TOS (Type of Service) **

The source host has received an ICMP message stating that "target host is unreachable due to the specified Type of Service."

Mitigation is not available for the alarm associated with this security event.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	Anomaly Index, High Concern Index
In what quantity?	• Anomaly Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_HOST_UNREACHABLE_FOR_SVC (301)

ICMP Net Unreach **

The source host has received an ICMP message that "the target network is unreachable."

Mitigation is not available for the alarm associated with this security event.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	High Recon Index, High Concern Index
In what quantity?	• High Recon Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_NETWORK_UNREACHABLE (289)

ICMP Net Unreach TOS **

The source host has received an ICMP message that the "network is unreachable for the specified Type Of Service."

Mitigation is not available for the alarm associated with this security event.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	Anomaly Index, High Concern Index
In what quantity?	• Anomaly Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_NETWK_UNREACHABLE_FOR_SVC (300)

ICMP Port Unreach **

The source host has received an ICMP message stating that "the destination port is unreachable." The designated transport protocol (e.g., UDP) is unable to demultiplex the datagram, but has no protocol mechanism to inform the sender.

Mitigation is not available for the alarm associated with this security event.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	High Recon Index, High Concern Index
In what quantity?	• High Recon Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_PORT_UNREACHABLE (292)

ICMP Precedence Cutoff **

The source host has received an ICMP message that "precedence cutoff" is in effect. The network operators have imposed a minimum level of precedence required for operation; the datagram was sent with a precedence below this level.

Mitigation is not available for the alarm associated with this security event.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	Anomaly Index, High Concern Index
In what quantity?	• Anomaly Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_PRECEDENCE_CUTOFF (304)

ICMP Proto (Protocol) Unreach **

The source host has received an ICMP message stating that "the destination protocol is unreachable."

Mitigation is not available for the alarm associated with this security event.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	Anomaly Index, High Concern Index
In what quantity?	• Anomaly Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_PROTOCOL_UNREACHABLE (291)

ICMP Received

What is the security event?

Questions about this event	Response
What does it mean when it triggers?	This indicates that the target host is being targeted in a DoS attack or a misconfigured network application.
What are next steps?	Determine how many ICMP packets are being received at what rate, when they were received, and from where they are coming. An ideal way to investigate this is to perform a flow query for the target host. Set the start time of the query to five minutes before the start time of the associated security event, and set the end time to the end time of the alarm (if there is an alarm). Set the protocol filter to *ICMP only*. Once the results have returned, find where the most ICMP packets came from during the searched time period. If the subject of the event is the client host in its ICMP-heavy flows, you can sort on Client Packets or Client Packet Rate (pps). The goal is to find the standout flow(s). After finding the standout flow(s), determine whether or not this is expected behavior.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	
In what quantity?	
What alarm categories does this security event contribute to for the target?	High Ddos Target Index, High Target Index
In what quantity?	• High Ddos Target Index: True • TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_ICMP_RECEIVED (50)

ICMP Src (Source) Host Isolated **

The source host has received an ICMP message that a "source host isolated error" has occurred.

Mitigation is not available for the alarm associated with this security event.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	High Recon Index, High Concern Index
In what quantity?	• High Recon Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_SOURCE_HOST_ISOLATED (297)

ICMP Src (Source) Route Failed **

The source host has received an ICMP message stating that a "source route failed" error has occurred.

Mitigation is not available for the alarm associated with this security event.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	Anomaly Index, High Concern Index
In what quantity?	• Anomaly Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

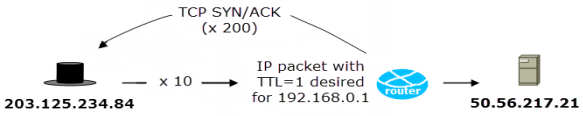
What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_SOURCE_ROUTE_FAIL (294)

ICMP Timeout

Mitigation is not available for the alarm associated with this security event.

ICMP_Timeout



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope	50.56.217.21	<CI value>*	ICMP_Timeout(10)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	It searches for the ICMP_TIME_EXCEEDED message generated as a result of the Traceroute tool, malfunctioning network devices (routing loops, etc), and firewalking techniques (using ICMP timeouts to determine ACLs allowed layer 4 protocols).
What does it mean when it triggers?	The host is potentially scanning / mapping the network to determine which layer 4 protocols are allowed through gateways/firewalls, etc.
What are next steps?	Determine if the host has been scanning ports along with the ICMP invocation. Run reports that show peers by port and protocol to discern a pattern of ICMP as well as various ports, usually repeating across peers. Determine whether or not data patterns being sent from the host is expected behavior (security tool/device, etc).
Non-standard flow data required?	For analyzing Netflow, a FlowSensor is required.

Questions about this event	Response
(FlowSensor, proxy, firewall, etc.)	
Notes	None

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	
Which policies have this event on by default?	Inside Hosts, Outside Hosts
Which policies have this event off by default?	
Which policies have this alarm on by default?	
Which policies have this alarm off by default?	Inside Hosts, Outside Hosts
Can you tune this event?	no
Is the event variance-based, threshold-based, or other?	N/A
What are default values and units?	N/A
Tolerance	N/A
Minimum threshold value	N/A

Questions about event	Response
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	
If so, what is it?	

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host that is the packet's destination
What is the target?	The host that is the packet's source
Which policy causes the event to trigger?	
What alarm categories does this security event contribute to for the source?	
In what quantity?	• High Recon Index: True

Questions about event	Response
	• CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	• TI: True

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: View details Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source & target IP, a time range five minutes before the event's first active time until the event's last active time, and ICMP. Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_ICMP_TO (258)

Inside Tor Entry Detected

What is the security event?

Questions about this event	Response
What does it mean when it triggers?	Tor, formerly The Onion Router, is a network used for anonymizing Internet connections which works by sending a connection through multiple relays before exiting the Tor network. A Tor entry node is the first server a Tor connection transits through before navigating and exiting the Tor network. This security event involves a host that is being monitored by Secure Network Analytics and is being advertised as a Tor entry node. Hosting a Tor entry node is not necessarily an issue, however it's almost certainly not something that should be occurring without a network's administrators being aware. Unlike a Tor exit node, Tor entry nodes only forward traffic within the Tor network, so the main concern is usually bandwidth.
What are next steps?	The main goal of investigating this event is largely non-technical. Determine whether or not anyone is aware of the Tor entry node and if it is permitted. If so, disable the event for the specific permitted host. You can also view the host's security event history to find out when it began to communicate while being advertised as a Tor entry node.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	High Policy Violation Index, High Concern Index
In what quantity?	• High Policy Violation Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_TOR_ENTRY_INSIDE_HOST (515)

Inside Tor Exit Detected

What is the security event?

Questions about this event	Response
What does it mean when it triggers?	Tor, formerly The Onion Router, is a network used for anonymizing Internet connections which works by sending a connection through multiple relays before exiting the Tor network. A Tor exit node is the last relay through which a Tor connection exits the Tor network, and it is what the destination of a network connection ultimately see as as the source of the connection. This security event involves a host that is being monitored by Secure Network Analytics and is being advertised as a Tor exit node. Hosting a Tor exit node is not necessarily an issue, however it's almost certainly not something that should be occurring without a network's administrators being aware. Concerns about hosting a Tor exit node often includes bandwidth usage and potential legal concerns around the activity being proxied through the node.
What are next steps?	The main goal of investigating this event is largely non-technical. Determine whether or not anyone is aware of the Tor exit node and if it is permitted. If so, disable the event for the specific permitted host. You can also view the host's security event history to find out when it began to communicate while being advertised as a Tor exit node. In addition, you can run a Top Peers report to view the amount of bandwidth the server has consumed as well as where that bandwidth has been going.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	High Policy Violation Index, High Concern Index
In what quantity?	• High Policy Violation Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_TOR_EXIT_INSIDE_HOST (319)

Low Traffic

The host's traffic average over the last 5 minutes has fallen below the minimum acceptable values.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	Anomaly Index, High Concern Index
In what quantity?	• Anomaly Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_LOW_TRAFFIC (29)

MAC Address Violation

The host has changed its MAC address more than an acceptable number of times since the last archive hour.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	High Policy Violation Index, High Concern Index
In what quantity?	• High Policy Violation Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_MAC_ADDRESS (25)

Mail Rejects

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	It searches for excess Mail Rejected messages from hosts that are not SMTP (mail) servers.
What does it mean when it triggers?	A host has received a number of Mail Rejected messages that exceed the threshold and the host is not a mail server. These messages may occur for a number of reasons. For example, the sending server/IP is registered as a spam server and the intended mail recipient is no longer available.
What are next steps?	Determine whether the host is intended to be sending/receiving mail. Run a Top Peers report by Port / Protocol (25/SMTP) to see who the server has been communicating with. If the host is intended to be sending/receiving mail, check the SMTP configurations to ensure they are correct. Check the larger spam and mail blacklists to see if the host IP is listed. If the server is not intended to send and receive email, investigate the host to see when the services were installed and if it was compromised in order to accomplish this.
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	A Flow Sensor is required to analyze NetFlow.
Notes	N/A

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	
Which policies have this event on by default?	Inside Hosts
Which policies have this event off by default?	Outside Hosts
Which policies have this alarm on by default?	Inside Hosts
Which policies have this alarm off by default?	Outside Hosts
Can you tune this event?	Yes
Is the event variance-based, threshold-based, or other?	Five-minute periods with Email Reject alerts to trigger alarm: Default to 5. Rejected email deliveries in 5 minutes to trigger alarm: Default to 5.
What are default values and units?	
Tolerance	N/A
Minimum threshold value	N/A
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	

Questions about event	Response
Is event tunable outside of the normal policy editor	
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	
If so, what is it?	

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host that is being scanned
What is the target?	No target host
Which policy causes the event to trigger?	
What alarm categories does this security event contribute to for the source?	
In what quantity?	• High Policy Violation Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: View details Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source IP, the start time (reset hour) of the event's active day until the event’s last active time and 25/TCP. Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_MAIL_REJECTS (12)

Mail Relay

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	It searches for hosts that have accumulated a high volume of email traffic, both inbound and outbound, and are sending larger volumes of email than they are receiving.
What does it mean when it triggers?	The host is potentially being used as a mail relay. If a mail server is not configured to use authentication, it is left open to the outside world with the SMTP port (25) open and/or does not have configurations to limit the networks that can relay mail. It may be taken advantage of by spammers.
What are next steps?	Determine the volume of email that is normal and whether the host is intended to send and receive email. If the server is intended to send and receive email, verify the SMTP server configurations. Enable authentication and network relay limits if they are not already enabled. If the server is not intended to send and receive email, investigate the host to see when the services were installed and whether the host was compromised to accomplish this.
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	A Flow Sensor is required to analyze NetFlow.
Notes	N/A

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	
Which policies have this event on by default?	Inside Hosts
Which policies have this event off by default?	Outside Hosts
Which policies have this alarm on by default?	Inside Hosts
Which policies have this alarm off by default?	Outside Hosts
Can you tune this event?	Yes
Is the event variance-based, threshold-based, or other?	Five-minute periods with Email Alerts to trigger alarm: Default to 5.
What are default values and units?	N/A
Tolerance	N/A
Minimum threshold value	N/A
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A

Questions about event	Response
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	
If so, what is it?	

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host being scanned
What is the target?	No target host
Which policy causes the event to trigger?	
What alarm categories does this security event contribute to for the source?	
In what quantity?	• High Policy Violation Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: View details Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source IP, the start time (reset hour) of the event's active day until the event’s last active time and 25/TCP. Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_MAIL_RELAY (10)

Max Flows Initiated

What is the security event?

Questions about this event	Response
What does it mean when it triggers?	This can indicate several different issues, but you should first determine if this is a sign of reconnaissance or a host engaging in a DoS attack.
What are next steps?	Determine what is causing these types flows by finding a common link between them. For example, are most of these flows going to the same host? Are they going to different hosts using the same port? An ideal way to determine this is to run one of the top reports. You can start with either the Top Peers report or Top Ports report. Access the report and then, on the Hosts tab in the Filter dialog, set the Direction field to *Total*, where *Client* is the source of the event and there are no exclusions for *Server Host*. On the Date/Time tab set the time period to five minutes before the start active time of the event up to the start active time of the event. On the Advanced tab, sort by *Flows*. Determine if the majority of the flows applies to a certain set of rows. (If this is not the case, run the other of the two suggested Top reports.) After finding the standout ports or peers, determine whether or not this is expected behavior.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	Anomaly Index, High Concern Index
In what quantity?	• Anomaly Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_MAX_FLOWS_INIT (17)

Max Flows Served

What is the security event?

Questions about this event	Response
What does it mean when it triggers?	This can indicate several different issues, but you should first determine if this is a sign of reconnaissance or a host being targeted in DoS attacks. For hosts that normally serve large volumes of traffic, it may just be an increase in normal use depending on threshold and tolerance settings.
What are next steps?	Determine what is causing these types flows by finding a common link between them. For example, are most of these flows coming from the same host? Are they coming from different hosts targeting the same port? An ideal way to determine this is to run one of the top reports. You can start with either the Top Peers report or Top Ports report. Access the report and then, on the Hosts tab in the Filter dialog, set the Direction field to *Total*, where *Server Host* is the source of the event and there are no exclusions for *Client*. On the Date/Time tab set the time period to five minutes before the start active time of the event up to the start active time of the event. On the Advanced tab, sort by *Flows*. Determine if the majority of the flows applies to a certain set of rows. (If this is not the case, run the other of the two suggested Top reports.) After finding the standout ports or peers, determine whether or not this is expected behavior.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	
In what quantity?	
What alarm categories does this security event contribute to for the target?	Anomaly Index, High Target Index
In what quantity?	• Anomaly Index: True • TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_MAX_FLOWS_SERVED (37)

New Flows Initiated

What is the security event?

Questions about this event	Response
What does it mean when it triggers?	This can indicate several different issues, but you should first determine if this is a sign of reconnaissance or a host engaging in a DoS attack.
What are next steps?	Determine what is causing these types flows by finding a common link between them. For example, are most of these flows going to the same host? Are they going to different hosts using the same port? An ideal way to determine this is to run one of the top reports. You can start with either the Top Peers report or Top Ports report. Access the report and then, on the Hosts tab in the Filter dialog, set the Direction field to *Total*, where *Client* is the source of the event and there are no exclusions for *Server Host*. On the Date/Time tab set the time period to five minutes before the start active time of the event up to the start active time of the event. On the Advanced tab, sort by *Flows*. Determine if the majority of the flows applies to a certain set of rows. (If this is not the case, run the other of the two suggested Top reports.) After finding the standout ports or peers, determine whether or not this is expected behavior.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	Anomaly Index, High Concern Index
In what quantity?	• Anomaly Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_NEW_FLOWS_INIT (18)

New Flows Served

What is the security event?

Questions about this event	Response
What does it mean when it triggers?	This can indicate several different issues, but you should first determine if this is a sign of reconnaissance or a host being targeted in DoS attacks. For hosts that normally serve large volumes of traffic, it may just be an increase in normal use depending on threshold and tolerance settings.
What are next steps?	Determine what is causing these types flows by finding a common link between them. For example, are most of these flows going to the same host? Are they going to different hosts using the same port? An ideal way to determine this is to run one of the top reports. You can start with either the Top Peers report or Top Ports report. Access the report and then, on the Hosts tab in the Filter dialog, set the Direction field to *Total*, where *Server Host* is the source of the event and there are no exclusions for *Client*. On the Date/Time tab set the time period to five minutes before the start active time of the event up to the start active time of the event. On the Advanced tab, sort by *Flows*. Determine if the majority of the flows applies to a certain set of rows. (If this is not the case, run the other of the two suggested Top reports.) After finding the standout ports or peers, determine whether or not this is expected behavior.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based,	

Questions about event	Response
threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	
In what quantity?	
What alarm categories does this security event contribute to for the target?	High Ddos Target Index, High Target Index
In what quantity?	• High Ddos Target Index: True • TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_NEW_FLOWS_SERVED (38)

New Host Active

A new host has been detected.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

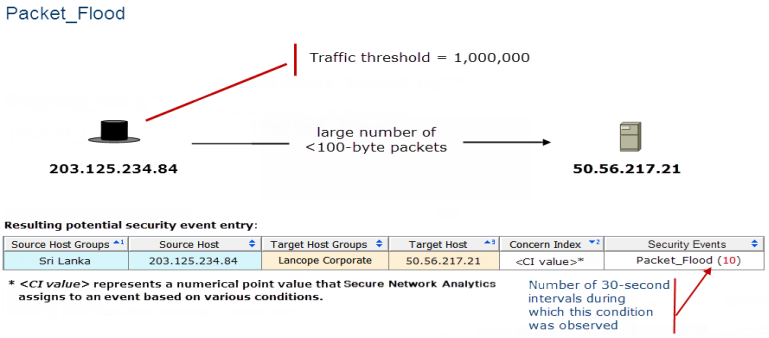
How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	High Policy Violation Index, High Concern Index
In what quantity?	• High Policy Violation Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_NEW_HOST (14)

Packet Flood



What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	It looks for a large volume of small-sized packets being sent over a long period of time to a host or hosts that are not SYN Flood attacks. (A SYN Flood attack occurs when a three-way TCP handshake is not completed, which then leaves the TCP connection open).
What does it mean when it triggers?	The source is sending out a large volume of packets, where each packet is smaller in size than a traditional TCP packet. This is occurring over a long period of time, indicating that the source is attempting a DoS (Denial of Service) or Brute Force attack against the target.
What are next steps?	Run a Top Peers report on the source to see if it has executed any similar flows, perhaps slightly shorter in length and close in size to other hosts. This can be a precursor to the attack, as the attacker is trying to gauge resources on various machines and identify weak targets. Run a Top Peers report on the target to see if any other machines have been compromised or re-purposed to join in the attack but have not yet reached the timing threshold for the alarm to fire.

Questions about this event	Response
	Investigate the source to see if the flow activity is behaving as expected. Configure DoS mitigation on the targets, if possible.
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	A Flow Sensor is required to analyze NetFlow.
Notes	N/A

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	
Which policies have this event on by default?	Inside Hosts, Outside Hosts
Which policies have this event off by default?	
Which policies have this alarm on by default?	Inside Hosts, Outside Hosts
Which policies have this alarm off by default?	
Can you tune this event?	Yes
Is the event variance-based, threshold-based, or other?	This alarm is triggered when the PPS is greater than 75,000 for Inside Hosts. or when the PPS is greater than 50,000 for Outside Hosts.

Questions about event	Response
What are default values and units?	
Tolerance	N/A
Minimum threshold value	N/A
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	
If so, what is it?	

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The attacker sending the short packets.
What is the target?	The receiver of the packets.
Which policy causes the event to trigger?	

Questions about event	Response
What alarm categories does this security event contribute to for the source?	High Ddos Source Index, High Concern Index
In what quantity?	• High Ddos Source Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	• High Ddos Target Index: True • TI: True

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: Target Host is X. Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source & target IP and a time range five minutes before the event's first active time until the event's last active time. Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

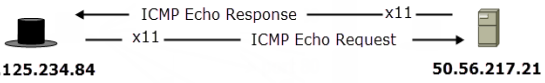
Questions about event	Response
What is the event ID?	SEC_ID_PACKET_FLOOD (8)

Ping

The source host has sent an ICMP echo reply and has received an ICMP echo response from the target.

Mitigation is not available for the alarm associated with this security event.

Ping



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope Corporate	50.56.217.21	<CI value>*	Ping(11)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	High Recon Index, High Concern Index
In what quantity?	• High Recon Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

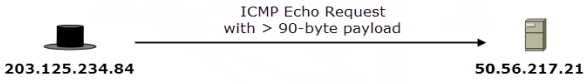
What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_PING_PROBE (257)

Ping Oversized Packet

Mitigation is not available for the alarm associated with this security event.

Ping_Oversized_Packet



Ping_Oversized_Packet events also apply to ICMP Echo Replies

Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope Corporate	50.56.217.21	<CI value>*	Ping_Oversized_Packet(58)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	It searches for ICMP packets that are larger than the standard size of 90 bytes, either as an ICMP echo request (if the host is the destination of the packet) or as an ICMP echo reply (if the host is the source of the packet).
What does it mean when it triggers?	This may indicate that a covert channel for data exfiltration or secretive communication is being used. ICMP is used for standard control or error response purposes, but it can be tunneled through to send and receive other data.
What are next steps?	Run a Top Services report to distinguish the excessive ICMP traffic from the all the other traffic sent to and from the host. Investigate the source and target hosts to see if unauthorized services are running. For example, a program or service must be running on the host, target, or both to capture or send the ICMP traffic. Run a Top Peers report filtered by the ICMP application (see note below) to see if the source or target have

Questions about this event	Response
	been communicating with other peers over excessive ICMP or to unfavorable peers outside the network (data exfiltration). Filter the report by ICMP for the Applications **Note:** When configuring the Top Peers report, in the Connection section, click **Select** under Applications.
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	None
Notes	None

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	
Which policies have this event on by default?	Inside Hosts, Outside Hosts
Which policies have this event off by default?	
Which policies have this alarm on by default?	
Which policies have this alarm off by default?	Inside Hosts, Outside Hosts
Can you tune this event?	No

Questions about event	Response
Is the event variance-based, threshold-based, or other?	N/A
What are default values and units?	N/A
Tolerance	N/A
Minimum threshold value	N/A
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	
If so, what is it?	

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host that sent the packet

Questions about event	Response
What is the target?	The host that received the packet
Which policy causes the event to trigger?	
What alarm categories does this security event contribute to for the source?	
In what quantity?	• High Command And Control Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	• TI: True

What information is available in Secure Network Analytics?

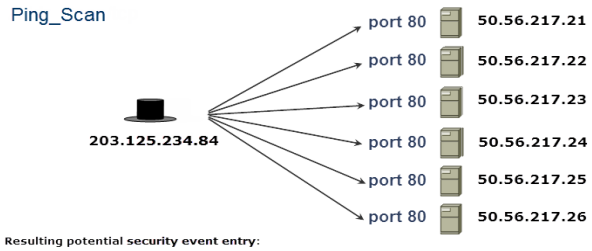
Questions about event	Response
What information is displayed in the alarm details?	Manager: View details Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source & target IP, the start time (reset hour) of the event's active day until the event’s last active time, and ICMP. Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_LONG_PING (278)

Ping Scan

Mitigation is not available for the alarm associated with this security event.



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope Corporate	50.56.217.21	<CI value>*	Ping_Scan(72)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	The scanning event is recorded and the alarm is triggered if the following is true: 1) the timeout is exceeded for an ICMP datagram; 2) it is not a service request; 3) the source host is not the destination host; 4) the source/destination port is not 38293 (used for Norton AV Host Discovery).
What does it mean when it triggers?	An ICMP scan is generally an early type of reconnaissance since, unlike scans of a particular port across hosts or many ports on one host, it is simply searching for any responsive host rather than a particular service. A host ping scanning is generally just trying to find other active hosts on a network, possibly for further investigation.
What are next steps?	Determine what the host was scanning. Since this is an ICMP-based scan, your main goal is to figure out which hosts are being scanned rather than what particular services are being targeted, as you would with a UDP or TCP scan. You can investigate this by performing a flow query where the client host or server host is the source of the event, the time period is the day of the

Questions about this event	Response
	event, and the protocol is ICMP. Sort the results by IP or host group of the peer to try to determine whether or not there is a pattern to the hosts being scanned.
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	For Flow Collector NetFlow edition, a Flow Sensor is required. For Flow Collector SFlow edition, nothing extra is required.
Notes	none

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	
Which policies have this event on by default?	Inside Hosts, Outside Hosts
Which policies have this event off by default?	
Which policies have this alarm on by default?	
Which policies have this alarm off by default?	Inside Hosts, Outside Hosts
Can you tune this event?	No
Is the event variance-based, threshold-based, or other?	N/A

Questions about event	Response
What are default values and units?	N/A
Tolerance	N/A
Minimum threshold value	N/A
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	
If so, what is it?	

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host that performs the scan
What is the target?	The host that is being scanned
Which policy causes the event to trigger?	

Questions about event	Response
What alarm categories does this security event contribute to for the source?	
In what quantity?	• High Recon Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: View details. Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source IP, the target's natural class C network (/24), the start time (reset hour) of the event's active day until the event’s last active time, and ICMP. Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_PING_ADDR_SCAN (277)

Port Scan

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	Port Scan counts how many target ports under or equal to 1024 one host talks on to another host. When the configurable threshold of target ports is crossed, the event is triggered.
What does it mean when it triggers?	It means that a host has been observed "port scanning" another host. This means that the scanning host is attempting to identify which services the scanned host can provide. When this is done by an outside host, it can be the precursor to attempts at exploitation; scanning from the internet, however, is to be expected. When the scanning host is an inside host, it can be a sign of either an attacker or a compromised host trying to move laterally within an organization's network.
What are next steps?	If the source host of this security event is an outside host, check to see if it has had continued communication with the host that it scanned. To do this, open a flow query between the source and target host. It may also be wise to simply view all traffic between the source host and your network. If the source of this host is an inside host, view the flows between the source and target using a Flow Query to determine whether or not this is expected behavior.
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	None
Notes	The source port will likely be over or equal to port 1024.

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	Port scan must be enabled on host performing the scan
Which policies have this event on by default?	Inside Hosts, Outside Hosts
Which policies have this event off by default?	None
Which policies have this alarm on by default?	None
Which policies have this alarm off by default?	Inside Hosts, Outside Hosts
Can you tune this event?	Yes
Is the event variance-based, threshold-based, or other?	Threshold based
What are default values and units?	N/A
Tolerance	N/A
Minimum threshold value	N/A
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	Yes
If so, what are its tunable attributes and units?	The tunable parameter is the number of scanned ports required to fire, and the default is 10.

Questions about event	Response
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	N/A
If so, what is it?	N/A

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host performing the scan
What is the target?	The host being scanned
Which policy causes the event to trigger?	The source host
What alarm categories does this security event contribute to for the source?	High Recon Index, High Concern Index
In what quantity?	• High Recon Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: View details. Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source & target IP and the start time (reset hour) of the event's active day until the event’s last active time. Desktop Client: Flows are filtered by time period of last five minutes.

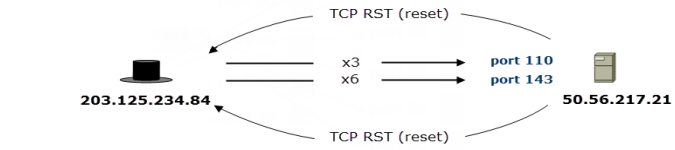
What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_PORT_SCAN (55)

Reset/tcp

Mitigation is not available for the alarm associated with this security event.

Reset/tcp



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope	50.56.217.21	<CI value>*	Reset/tcp-110(3) Reset/tcp-143(6)

*** *<CI value>* represents a numerical point value that the Secure Network Analytics engine assigns to an event based on various conditions.**

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	It searches for TCP Reset packets coming from a target port that 1) is not used for HTTP; 2) has not had TCP activity on it; 3) has an ICMP type of "Destination Unreachable"; 4) is not SNMP; and 5) is not using unprivileged ports (1024+).
What does it mean when it triggers?	TCP Reset packets are sent when a TCP conversation is torn down or when there is a problem with the conversation. These can be sent by malfunctioning devices in the middle of a conversation (such as load balancers), or they can be sent by the target if a port is not open or available. In the case of the latter, if multiple ports are responding this way and are in groups or are congruent, it usually indicates a network scan is being performed to determine which services, if any, are available on a host.
What are next steps?	Run a Top Peers report for the source to determine if there is a pattern to the ports that are being used in the flows. Determine whether the source is a security host, device, or appliance that has been authorized to scan.

Questions about this event	Response
	If not, investigate the host for scanning software or services, as well as evidence of compromise.
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	A Flow Sensor is required to analyze NetFlow.
Notes	None

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	
Which policies have this event on by default?	Inside Hosts, Outside Hosts
Which policies have this event off by default?	
Which policies have this alarm on by default?	
Which policies have this alarm off by default?	Inside Hosts, Outside Hosts
Can you tune this event?	No
Is the event variance-based, threshold-based, or other?	N/A
What are default values and	N/A

Questions about event	Response
units?	
Tolerance	N/A
Minimum threshold value	N/A
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	
If so, what is it?	

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host that is the packet's destination
What is the target?	The host that is the packet's source
Which policy causes the event to trigger?	

Questions about event	Response
What alarm categories does this security event contribute to for the source?	
In what quantity?	• High Recon Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	• TI: True

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: View details Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source & target IP, a time range five minutes before the event's first active time until the event's last active time, the associated port as <port>/TCP, and TCP. Desktop Client: Flows are filtered by time period of last five minutes.

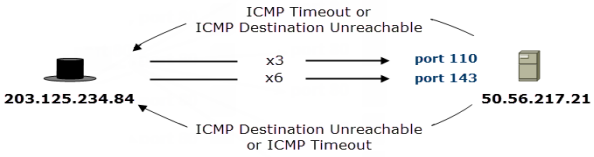
What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_TCP_PROBE (262)

Reset/udp

Mitigation is not available for the alarm associated with this security event.

Reset/udp



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope	50.56.217.21	<CI value>*	Reset/udp-110(3) Reset/udp-143(6)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	It searches for UDP Reset packets coming from a target port that 1) is not used for HTTP; 2) has not had UDP activity on it; 3) has an ICMP type of "Destination Unreachable"; 4) is not SNMP; and 5) is not using unprivileged ports (1024+).
What does it mean when it triggers?	UDP Reset packets are sent when communication to a UDP port that is closed or not available has been attempted. These packets can be sent by malfunctioning devices in the middle of a conversation or they can be sent by the target if a port is not open or available. In the case of the latter, if multiple ports are responding this way and are in groups or are congruent, it usually indicates a network scan is being performed to determine which services, if any, are available on a host.
What are next steps?	Run a Top Peers report for the source to determine if there is a pattern to the ports that are being used in the flows. Determine whether the source is a security host, device, or appliance that has been authorized to scan.

Questions about this event	Response
	If not, investigate the host for scanning software or services, as well as evidence of compromise.
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	A Flow Sensor is required to analyze NetFlow.
Notes	None

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	
Which policies have this event on by default?	Inside Hosts, Outside Hosts
Which policies have this event off by default?	
Which policies have this alarm on by default?	
Which policies have this alarm off by default?	Inside Hosts, Outside Hosts
Can you tune this event?	No
Is the event variance-based, threshold-based, or other?	N/A
What are default values and	N/A

Questions about event	Response
units?	
Tolerance	N/A
Minimum threshold value	N/A
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	
If so, what is it?	

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host that is the packet's destination
What is the target?	The host that is the packet's source
Which policy causes the event to trigger?	

Questions about event	Response
What alarm categories does this security event contribute to for the source?	
In what quantity?	• High Recon Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	• TI: True

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: View details Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source & target IP, a time range one minute before the event's first active time until the event's last active time, the associated port as <port>/UDP, and UDP. Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_UDP_PROBE (261)

Scanner Talking

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	A host that has been scanning your network now has a two-way conversation with one of the target hosts that it scanned. It is enabled by default in both the Inside Hosts policy and the Outside Hosts policy. It is, however, disabled by default in the Network Management Scanners role policy.
What does it mean when it triggers?	A machine which has been flagged as an address scanner is communicating with one of the machines that has been scanned. If the source is not an authorized scanner, it can indicate the scanner has found a target matching its attack vector and has successfully compromised it.
What are next steps?	Determine whether the source is an authorized scanner. If the source is not an authorized scanner, run a Peer report for the source to see other hosts communicated to, making sure to choose peers that have increased flows or flow sizes. Investigate the source and target for signs of compromise.
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	
Notes	

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	
Which policies have this event on by default?	Inside Hosts, Outside Hosts
Which policies have this event off by default?	none
Which policies have this alarm on by default?	Inside Hosts, Outside Hosts
Which policies have this alarm off by default?	none
Can you tune this event?	no
Is the event variance-based, threshold-based, or other?	N/A
What are default values and units?	N/A
Tolerance	N/A
Minimum threshold value	N/A
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A

Questions about event	Response
Is event tunable outside of the normal policy editor	lc_threshold value addr_scan_talking_stale_timeout controls the amount of time before the global scan list is reset.
If so, what are the alternate locations of tunable values?	none
Does event have a default mitigation?	
If so, what is it?	

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The scanner that is communicating
What is the target?	The scanned host that is being communicated with
Which policy causes the event to trigger?	The source host policy
What alarm categories does this security event contribute to for the source?	
In what quantity?	• Attack Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	• TI: True

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: View details Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source & target IP, a time range five minutes before the event's first active time until the event's last active time, and client bytes & server bytes (both of which are greater than or equal to 1). Desktop Client: Flows between the client and the server, starting at the alarm time.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_ADDR_SCAN_TALKING (63)

Slow Connection Flood

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	The source host has sent an excessive number of simultaneous connections to a single destination. Each connection has a very low packet-per-second rate.
What does it mean when it triggers?	Indicates that a host is initiating multiple connections to a target with a very low packet rate. The goal of connections like these are to maintain open connections without requiring much bandwidth. This is a type of application denial-of-service (DoS) attack which can render a service unavailable without requiring a large amount of bandwidth, which makes the attack easier to carry out against a vulnerable host and often more difficult to detect.
What are next steps?	The goal is to determine if the connections to the target are legitimate and if the target experiences any performance degradation. While it is possible that this can be malicious behavior between two inside hosts, the event is more likely to be interesting between an inside and an outside host. First, run a flow query between the source and target of the event for the day of the event. Take note of whether the flow is ongoing. If it is not, and there was no service outage, it was likely not an issue. You can also check the security event history of both the source and target hosts. Does the source host have this event against multiple targets or historically? If so, this is something to research further. Does the target host have many hosts triggering this event against it at once but not historically? This may be sign of a distributed denial-of-servce (DDoS) attack. If the event is also firing historically, it may just be normal behavior for whatever application the

Questions about this event	Response
	service is hosting. If this is the case, consider turning t he event off for the particular host. If the relevant traffic was observed by a Flow Sensor, run a performance report to see if the SRT (Server Response Time) has been affected due to the nature of the traffic. This could indicate whether or not this is legitimate traffic.
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	None
Notes	None

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	
Which policies have this event on by default?	Inside Hosts, Outside Hosts
Which policies have this event off by default?	
Which policies have this alarm on by default?	Outside Hosts
Which policies have this alarm off by default?	
Can you tune this event?	Yes

Questions about event	Response
Is the event variance-based, threshold-based, or other?	Threshold
What are default values and units?	N/A
Tolerance	N/A
Minimum threshold value	30
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	Yes
If so, what are its tunable attributes and units?	The number of slow connections needed to trigger the alarm
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	
If so, what is it?	

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host sending the excessive number of slow connections
What is the target?	The host receiving the excessive number of slow

Questions about event	Response
	connections
Which policy causes the event to trigger?	
What alarm categories does this security event contribute to for the source?	
In what quantity?	• High Ddos Source Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	• High Ddos Target Index: True • TI: True

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: The target host X has observed Y low-pps connections using port Z. Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source & target IP, a time range two minutes before the event's first active time until the event's last active time, the ports 80/TCP, 443/TCP, and 8080/TCP.

Questions about event	Response
	Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_SLOW_CONNECTION_FLOOD (44)

Spam Source

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	It is searching for sources with an excessive volume of outgoing email or for an excessive address-to-message ratio (i.e., many recipients per single message).
What does it mean when it triggers?	It can indicate that a server is being used to send spam email. This can be accomplished through compromise or misconfiguration. This can cause public IPs to be blocked by blacklists and spam lists.
What are next steps?	Determine if the source is intended to send and receive email. If the source is not meant to do so, determine when the increase in volume of outgoing email began. Search for signs of compromise or malicious software installation around that time. If the source is intended to send and receive email, determine when the source first appeared on the network and search for signs of compromise.
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	A Flow Sensor is required to analyze NetFlow.
Notes	N/A

What policy settings are available for this security event?

Questions about event	Response
What policy settings are	

Questions about event	Response
required for this security event to trigger?	
Which policies have this event on by default?	Inside Hosts
Which policies have this event off by default?	Outside Hosts
Which policies have this alarm on by default?	Inside Hosts
Which policies have this alarm off by default?	Outside Hosts
Can you tune this event?	Yes
Is the event variance-based, threshold-based, or other?	Five-minute periods with Spam Source alerts to trigger alarm: Default 5. Addresses per email for Spam Email alert: Default 10.
What are default values and units?	
Tolerance	N/A
Minimum threshold value	N/A
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A
Is event tunable outside of the normal policy editor	N/A

Questions about event	Response
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	
If so, what is it?	

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host that is being scanned
What is the target?	No target host
Which policy causes the event to trigger?	
What alarm categories does this security event contribute to for the source?	
In what quantity?	• High Policy Violation Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: View details Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source IP, the start time (reset hour) of the event's active day until the event's last active time, and 25/TCP. Desktop Client: Flows are filtered by time period of last five minutes.

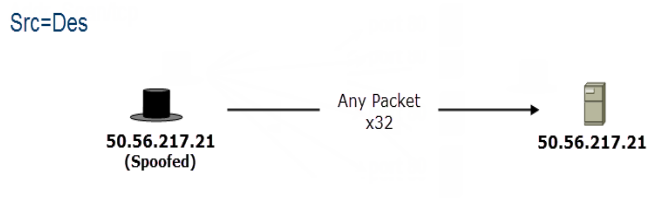
What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_SPAM_SOURCE (11)

Src=Des (Source=Destination)

The source and target hosts of an IP datagram are the same. This security event usually results from a crafted packet intended to disrupt routing.

Mitigation is not available for the alarm associated with this security event.



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	50.56.217.21	Lancope Corporate	50.56.217.21	<CI value>*	Src=Des(32)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	Anomaly Index
In what quantity?	• Anomaly Index: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_BOOMERANG (273)

SSH Reverse Shell

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	Detects an SSH session that appears to be a reverse shell. More data is being sent to the outside host than is being received.
What does it mean when it triggers?	The intent of this security event alarm is to find a reverse SSH shell. An attacker may use an SSH reverse shell as a method of establishing on-demand access to the compromised network through what looks like an outbound SSH connection. This allows an attacker to maintain access to a system even when incoming connections are blocked off by something like a firewall.
What are next steps?	When investigating this security event, it is important to keep the role of the source host, presumably on the inside network, in perspective. If the host in question is an SSH or SFTP server in an official capacity, this could be a false alarm, and further host policy tuning may be required to limit these alarms from such devices. However, in a situation where inside hosts do not have any obvious capacity as such a device, the identity of the outside host in question must be established. Is it owned by a well-known entity? If so, it could be a false alarm. If it is not a well-known entity, run a Top Peers (outbound) report on the target host. This report provides a list of inside peers sorted by the amount of data that have communicated with the outside host. This indicates whether or not it a very common peer within your environment and can potentially assist you in determining if this behavior is expected.
Non-standard flow data required?	None

Questions about this event	Response
(FlowSensor, proxy, firewall, etc.)	
Notes	None

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	
Which policies have this event on by default?	Inside Hosts, Outside Hosts
Which policies have this event off by default?	
Which policies have this alarm on by default?	
Which policies have this alarm off by default?	Inside Hosts, Outside Hosts
Can you tune this event?	Yes
Is the event variance-based, threshold-based, or other?	Threshold
What are default values and units?	N/A
Tolerance	N/A
Minimum threshold value	Traffic exceeds 10,000 bytes AND client data percentage exceeds 60.

Questions about event	Response
Maximum threshold value	Client data percentage exceeds 80.
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	
If so, what is it?	

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The inside host with traffic to an SSH port of an outside host
What is the target?	The outside host receiving SSH traffic
Which policy causes the event to trigger?	
What alarm categories does this security event contribute to for the source?	
In what quantity?	• High Command And Control Index: True

Questions about event	Response
	• CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	• TI: True

What information is available in Secure Network Analytics?

Questions about event	Response
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source & target IP, a time range five minutes before the event's first active time until the event's last active time, the port 22/TCP. Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_SSH_REV_SHELL (61)

Stealth Scan/tcp

Mitigation is not available for the alarm associated with this security event.

Stealth_Scan/tcp

Stealth_Scan/udp probes operate in the same manner as Stealth_Scan/tcp probes.

Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope	50.56.217.21	<CI value>*	Stealth_Scan/tcp-848(2) Stealth_Scan/tcp-231(1)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	The source host has used the same source port to connect to different ports on the target host at the same time. This behavior indicates applications that have used raw sockets to create TCP or UDP connections. The security event shows the last target port accessed before the security event was recognized.
What does it mean when it triggers?	N/A
What are next steps?	N/A
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	For Flow Collector NetFlow edition, a Flow Sensor is required. For Flow Collector sFlow edition, nothing extra is required.
Notes	N/A

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	
Which policies have this event on by default?	Inside Hosts, Outside Hosts
Which policies have this event off by default?	
Which policies have this alarm on by default?	
Which policies have this alarm off by default?	Inside Hosts, Outside Hosts
Can you tune this event?	no
Is the event variance-based, threshold-based, or other?	N/A
What are default values and units?	N/A
Tolerance	N/A
Minimum threshold value	N/A
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A

Questions about event	Response
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	
If so, what is it?	

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host that performs the scan
What is the target?	The host that is being scanned
Which policy causes the event to trigger?	
What alarm categories does this security event contribute to for the source?	
In what quantity?	'1' Policy: • CI: True '8000' Policy: • High Recon Index: True • CI: True
What alarm categories does this security event contribute to for the target?	

Questions about event	Response
In what quantity?	'1' Policy: • TI: True '8000' Policy: • TI: True

What information is available in Secure Network Analytics?

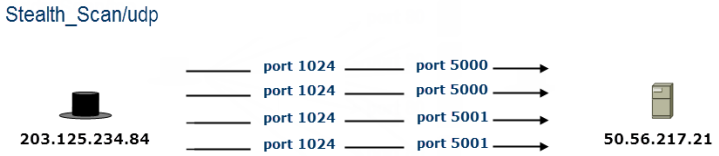
Questions about event	Response
What information is displayed in the alarm details?	Manager: View details. Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source & target IP, a time range five minutes before the event's first active time until the event's last active time, the associated port as <port>/TCP, and TCP. Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_TCP_STEALTH (272)

Stealth Scan/udp

Mitigation is not available for the alarm associated with this security event.



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope	50.56.217.21	<CI value>*	Stealth_Scan/udp-5000(2) Stealth_Scan/udp-5001(2)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	The event fires when Secure Network Analytics detects traffic which would not be generated naturally by an operating system, suggesting that someone is deliberately crafting packets in an attempt to evade detection.
What does it mean when it triggers?	N/A
What are next steps?	N/A
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	For Flow Collector NetFlow edition, a Flow Sensor is required. For Flow Collector sFlow edition, nothing extra is required.
Notes	N/A

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	
Which policies have this event on by default?	Inside Hosts, Outside Hosts
Which policies have this event off by default?	
Which policies have this alarm on by default?	
Which policies have this alarm off by default?	Inside Hosts, Outside Hosts
Can you tune this event?	no
Is the event variance-based, threshold-based, or other?	N/A
What are default values and units?	N/A
Tolerance	N/A
Minimum threshold value	N/A
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A

Questions about event	Response
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	
If so, what is it?	

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host that performs the scan.
What is the target?	The host that is being scanned
Which policy causes the event to trigger?	
What alarm categories does this security event contribute to for the source?	
In what quantity?	'1' Policy: • CI: True '8000' Policy: • High Recon Index: True • CI: True
What alarm categories does this security event contribute to for the target?	

Questions about event	Response
In what quantity?	'1' Policy: • TI: True '8000' Policy: • TI: True

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: View details. Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source & target IP, a time range one minute before the event's first active time until the event's last active time, the associated port as <port>/UDP, and UDP. Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_UDP_STEALTH (271)

Suspect Data Hoarding

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	Suspect Data Hoarding monitors how much TCP/UDP data an inside host, while acting as a client, downloads from other inside hosts in a reset period. The event fires when the amount of data surpasses the threshold for a given host. This threshold can either be built automatically by baselining or it can be set manually.
What does it mean when it triggers?	This event is potentially an indication of a particular host gathering data to prepare for exfiltration or other large-than-normal downloads of internal data.
What are next steps?	Determine how much data was downloaded and where that data was downloaded from. An ideal way to investigate this is to run a Top Peers (inbound) report. Set the time period of the query to be the day of the event. Filter the report so that *Client* or *Server Host* is the source IP of the security event and *Other Host* is the Inside Hosts host group. The goal is to find the standout peers who sent the majority of the data. After finding the standout peers, determine whether or not data being sent from these peers in the observed quantity is expected behavior.
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	N/A
Notes	N/A

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	The event must be enabled for Inside Host host group.
Which policies have this event on by default?	Inside Hosts, Outside Hosts
Which policies have this event off by default?	Firewalls, Proxies, & NAT Devices
Which policies have this alarm on by default?	None
Which policies have this alarm off by default?	Inside Hosts; Outside Hosts; Firewalls, Proxies, & NAT Devices
Can you tune this event?	Yes
Is the event variance-based, threshold-based, or other?	Variance or threshold-based.
What are default values and units?	
Tolerance	92
Minimum threshold value	500M client payload bytes in 24 hours.
Maximum threshold value	1T downloaded payload bytes in 24 hours.
Is event tunable with non-variance-based parameters?	Yes
If so, what are its tunable attributes and units?	The event can be set to trigger off a particular number of bytes that does not take baselines or tolerance into account.

Questions about event	Response
Is event tunable outside of the normal policy editor	No
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	No
If so, what is it?	N/A

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The inside host that is receiving the payload data.
What is the target?	The inside host or hosts that are sending the payload data.
Which policy causes the event to trigger?	The source's policy.
What alarm categories does this security event contribute to for the source?	High Data Hoarding Index, High Concern Index
In what quantity?	• High Data Hoarding Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: Observed W bytes. Expected X bytes, tolerance of Y allows up to Z bytes. Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source vs. Inside Hosts, the start time (reset hour) of the event's active day until the event's last active time, 53/UDP, 67/UDP, 68/UDP, 161/TCP, 161/UDP, 162/TCP, 162/UDP, client bytes & server bytes (both of which are greater than or equal to 1), and total bytes greater or equal to 1000. Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_SUSPECT_DATA_HOARD (315)

Suspect Data Loss

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	When this event triggers, an inside host acting as a client has uploaded a cumulative amount of TCP or UDP payload data to an outside host, and the cumulative amount exceeds the threshold value set in the policy applied to the inside host. This can be used as a variance-based alarm.
What does it mean when it triggers?	A host is being used to upload more information to the Internet than is acceptable. This can be anything from someone using external backup services to maliciously exfiltrating corporate data.
What are next steps?	Determine how much data was uploaded and where the bulk of that data went. An ideal way to determine this is to run a Top Peers (outbound) report on the host that was the source of the security event. Filter the report so that the client is the source of the event and the server host group is set to *Outside Hosts*. The goal is to find the standout peers who received the majority of the data. After finding the standout peers, determine whether or not data being received by these peers in the observed quantity is expected behavior.
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	No
Notes	N/A

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	This event must be enabled in policies applied to both the source and target hosts.
Which policies have this event on by default?	Inside Hosts, Outside Hosts, Client IP Policy
Which policies have this event off by default?	Firewalls, Proxies, & NAT Devices; Guest Wireless; Mail Server Policy; Trusted Internet Hosts
Which policies have this alarm on by default?	Inside Hosts, Outside Hosts, Client IP Policy
Which policies have this alarm off by default?	Firewalls, Proxies, & NAT Devices; Guest Wireless; Mail Server Policy; Trusted Internet Hosts
Can you tune this event?	Yes
Is the event variance-based, threshold-based, or other?	Variance or threshold-based
What are default values and units?	
Tolerance	50
Minimum threshold value	1G client payload bytes in 24 hours
Maximum threshold value	100G client payload bytes in 24 hours
Is event tunable with non-variance-based parameters?	Yes
If so, what are its tunable attributes and units?	The event can be set to trigger off a particular number of bytes that does not take baselines or tolerance into account.

Questions about event	Response
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	No
If so, what is it?	N/A

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The inside host, acting as a client, that is sending the payload data.
What is the target?	The outside host or hosts that are receiving the payload data from your inside host.
Which policy causes the event to trigger?	The source's policy.
What alarm categories does this security event contribute to for the source?	High Exfiltration Index, High Concern Index
In what quantity?	• High Exfiltration Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: Observed W bytes. Expected X bytes, tolerance of Y allows up to Z bytes. Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source IP and Outside Hosts and the start time (reset hour) of the event's active day until the event’s last active time. Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_DATA_LOSS (40)

Suspect Long Flow

What is the security event?

Questions about this event	Response
What does it mean when it triggers?	This security event detects long-established connections such as the ones used by remote desktop technologies and VPN, but it can also detect communication channels such as spyware, IRC botnets, and other covert means of communication. This event is not necessarily indicative of malicious behavior or compromise by itself, but it contributes to the identification of interesting hosts. When you perform an upgrade to your system, this security event should start firing again after 6 days.
What are next steps?	The goal is to determine if this traffic represents normal activity. Oftentimes you can do this by identifying the destination of the traffic. A good starting point is to pivot into the associated flow table for the security event to get more details of the flow such as source and destination IP addresses, ports, services, starting time of the flow, geo-location information, and username (if available). If the target is an outside host, run an external lookup to verify the owner of the IP. If the target is a known business partner or trusted network, you should classify the target into its corresponding group. If an external lookup of the host is not enough to identify it, run a Top Peer reports to identify other hosts communicating with the target to identify similar behaviors.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	High Command And Control Index, High Concern Index
In what quantity?	• High Command And Control Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_SUSPECT_LONG_FLOW (33)

Suspect Quiet Long Flow

What is the security event?

Questions about this event	Response
What does it mean when it triggers?	This security event identifies heartbeat connections that are used in some types of command and control (C&C) activity as well as other suspicious communication channels such as spyware, IRC botnets, and other covert means of communication. This event is similar to a beaconing host except that bidirectional communications are included, provided a low volume of data is transferred. Note that this event can also identify background website heartbeats.
What are next steps?	The goal is to determine if this traffic represents normal activity. Oftentimes you can do this by identifying the destination of the traffic. A good starting point is to pivot into the associated flow table for the security event to get more details of the flow such as source and destination IP addresses, ports, services, starting time of the flow, geo-location information, and username (if available). If the target is an outside host, run an external lookup to verify the owner of the IP. If the target is a known business partner or trusted network, you should classify the target into its corresponding group. If an external lookup of the host is not enough to identify it, run a Top Peer reports to identify other hosts communicating with the target to identify similar behaviors. You can also run a Flow Traffic report to visualize suspicious traffic patterns. Heartbeats to a C&C server will exhibit a periodic pattern with a low amount of bytes transferred.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	High Command And Control Index, High Concern Index
In what quantity?	• High Command And Control Index: True • CI: True
What alarm categories does this security event contribute to for the target?	High Target Index
In what quantity?	• TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_QUIET_LONG_DURATION_FLOW (48)

Suspect UDP Activity

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	The source host has been identified scanning multiple hosts on a UDP port and has successfully sent a large UDP packet to another previously scanned host. This type of behavior is consistent with many single-packet UDP-based worms such as "SQL Slammer" and "Witty." Investigate this security event immediately.
What does it mean when it triggers?	The source host has successfully sent a single, large UDP packet to one of the previously scanned hosts.
What are next steps?	Investigate this activity immediately, since it is most commonly identified with many UDP-based worms.
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	A Flow Sensor is required for acquiring and working with NetFlow.
Notes	N/A

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	
Which policies have this event on by default?	Inside Hosts, Outside Hosts
Which policies have this event	

Questions about event	Response
off by default?	
Which policies have this alarm on by default?	Inside Hosts, Outside Hosts
Which policies have this alarm off by default?	
Can you tune this event?	No
Is the event variance-based, threshold-based, or other?	N/A
What are default values and units?	N/A
Tolerance	N/A
Minimum threshold value	N/A
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	
If so, what is it?	

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host that sent the packet
What is the target?	The host being scanned and receiving the packet
Which policy causes the event to trigger?	
What alarm categories does this security event contribute to for the source?	
In what quantity?	• Attack Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	• TI: True

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: Source host is using X service (Y Protocol) as Peer to Z. Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source & target IP, a

Questions about event	Response
	time range 35 minutes before the event's first active time until the event's last active time, and the associated port as <port>/UDP. Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_SUSPECT_UDP_ACTIVITY (24)

SYN Flood

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	The source host has sent an excessive number of TCP connection requests (SYN packets) in a 5-minute period. This may indicate a Denial of Service (DoS) attack or non-stealthy scanning activity.
What does it mean when it triggers?	This indicates that the source host is engaged in a DoS attack (potentially caused by either a compromised host or driven by a user) or a misconfigured network application. Many SYN packets are often sent to consume a target's bandwidth as part of larger, distributed denial-of- service (DDoS) attacks. However, it is possible that an application is failing to establish a TCP connection and is trying to re-establish one at a very high rate. Relatively low packet counts relative to a large number of IPs is also likely to be a sign of reconnaissance.
What are next steps?	Determine how many SYNs are being sent at what rate, when they were sent, and where they are going. An ideal way to investigate this is to perform a flow query for the source host. Set the start time of the query to five minutes before the start time of the associated security event, and set the end time to the end time of the alarm (if there is an alarm). Once the results have returned, find where the most SYN packets went during the searched time period. If the subject of the event is the client host in its SYN- heavy flows, you can sort on Client SYN Packets, Client Packets, or Client Packet Rate (pps). The goal is to find the standout flow (s). After finding the standout flow(s), determine whether or not this is a misconfiguration. An Inside to Inside SYN Flood is often a misconfiguration; an Inside

Questions about this event	Response
	to Outside SYN Flood occasionally is.
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	None
Notes	N/A

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	
Which policies have this event on by default?	Inside Hosts, Outside Hosts
Which policies have this event off by default?	
Which policies have this alarm on by default?	Inside Hosts, Outside Hosts
Which policies have this alarm off by default?	
Can you tune this event?	Yes
Is the event variance-based, threshold-based, or other?	behavioral and threshold
What are default values and units?	N/A

Questions about event	Response
Tolerance	75
Minimum threshold value	10 SYN packets per period
Maximum threshold value	4 Million SYN packets per period
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	
If so, what is it?	

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host sending SYN Packets
What is the target?	None
Which policy causes the event to trigger?	
What alarm categories does this security event contribute to for the source?	High Ddos Source Index, High Concern Index

Questions about event	Response
In what quantity?	• High Ddos Source Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: Observed W pp5m. Expected X pp5m, tolerance of Y pp5m allows up to Z pp5m. Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source IP, a time range five minutes before the event's first active time until the event's last active time, and TCP. Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_SYN_FLOOD (5)

SYNs Received

What is the security event?

Questions about this event	Response
What does it mean when it triggers?	This indicates that the target host is being targeted in a DoS attack or misconfigured network application. Many SYN packets are often sent to consume a target's bandwidth as part of larger DDoS or DoS attacks. However, it is possible that an application is failing to establish a TCP connection and trying to re-establish one at a very high rate.
What are next steps?	Determine how many SYNs are being sent at what rate, when they were sent, and from where they are coming. An ideal way to investigate this is to perform a flow query for the target host. Set the start time of the query to five minutes before the start time of the associated security event, and set the end time to the end time of the alarm (if there is an alarm). Once the results have returned, find where the most SYN packets came from during the searched time period. If the target of the event is the server host in its SYN-heavy flows, you can sort on Client SYN Packets, Client Packets, or Client Packet Rate (pps). The goal is to find the standout flow(s). After you find the standout flow(s), determine whether or not this is a misconfiguration. An Inside to Inside SYN Flood is often a misconfiguration.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	
In what quantity?	
What alarm categories does this security event contribute to for the target?	High Ddos Target Index, High Target Index
In what quantity?	• High Ddos Target Index: True • TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_SYNS_RECEIVED (19)

Talks to Phantoms

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	Any time a flow exists where one host is sending non-trivial traffic to a host which has never communicated with anything, add the silent host to the "phantom list" of the host that is communicating. If the phantom list of a host grows past the configured allowable maximum, then trigger the event from the talking host to the most recently seen phantom host.
What does it mean when it triggers?	Since computers rarely attempt to send unsolicited traffic to hosts that do not exist, a host involved in such activity is noteworthy. It is possible that this is a sign of someone attempting to perform reconnaissance, however, it is also possible that a host has been misconfigured to talk to nonexistent hosts.
What are next steps?	This security event can be a little tricky to investigate since it is not possible today to specify "phantoms" as part of a flow query, but you can get close. The goal of the investigation is to find the flows that were sent to unresponsive hosts and draw meaning from the common thread between the flows. Find the unidirectional flows. Build a flow query where the time range is the day of the security event. Make the client host the source IP of the security event, and allow the server host to be any IP. Find the common thread between these flows. For example, were they all going to the same server port? Did they all occur at approximately the same time? Were they going to hosts that you know once existed? How many hosts were there? **In the Desktop Client:** In the Traffic tab, filter so that

Questions about this event	Response
	the number of server packets are less than or equal to 0 (leave the "Greater than or equal to" part of the setting empty). To make sure everything is captured, you should repeat this query where the source of the event is the server of the flow query, and client packets are less than or equal to 0. Note that this is unlikely to produce additional results too frequently. **In the Web App:** On the Flow Search page, in the Advanced Subject Options section, set the Packets field to **< 1** and the Orientation field to **Server**. To make sure everything is captured, you should repeat this query where the source of the event is the server of the flow query, and client packets are **< 1**. Note that this is unlikely to produce additional results too frequently.
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	None
Notes	N/A

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	
Which policies have this event on by default?	Inside Host, Outside Hosts
Which policies have this event off by default?	

Questions about event	Response
Which policies have this alarm on by default?	None
Which policies have this alarm off by default?	Inside Host, Outside Hosts
Can you tune this event?	Yes
Is the event variance-based, threshold-based, or other?	Threshold
What are default values and units?	N/A
Tolerance	N/A
Minimum threshold value	Three phantom hosts that a particular host has attempted to reach.
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	
If so, what is it?	

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host that attempts to talk to the phantom host(s).
What is the target?	The phantom host
Which policy causes the event to trigger?	
What alarm categories does this security event contribute to for the source?	
In what quantity?	• High Recon Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	• TI: True

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: View details. Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source IP, the start time (reset hour) of the event's active day until the event’s

Questions about event	Response
	last active time, and bytes & packets (both of which are less than 1). Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_TALKS_TO_PHANTOMS (59)

Target Data Hoarding

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	Target Data Hoarding monitors how much TCP/UDP data an inside host, while acting as a server, serves to other inside hosts in a reset period. The event fires when the amount of data surpasses the threshold for a given host. This threshold can either be built automatically by baselining or it can be set manually.
What does it mean when it triggers?	This event is potentially an indication of one or many Inside Hosts gathering more data than normal from a particular Inside Host, potentially in preparation for exfiltration or misuse.
What are next steps?	Determine how much data was transferred and where the bulk of that data went. An ideal way to determine this is to run a Top Peers (outbound) report on the host that was the source of the security event. Filter the report so that *Client* or *Server Host* is the target IP of the security event and *Other Host* is the Inside Hosts host group. The goal is to find the standout peers who received the majority of the uploaded data. After finding the standout peers, determine whether or not data being received by these peers in the observed quantity is expected behavior.
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	N/A
Notes	N/A

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	The event must be enabled for Inside Host host group.
Which policies have this event on by default?	Inside Hosts, Outside Hosts
Which policies have this event off by default?	Firewalls, Proxies, & NAT Devices
Which policies have this alarm on by default?	None
Which policies have this alarm off by default?	Inside Hosts; Outside Hosts; Firewalls, Proxies, & NAT Devices
Can you tune this event?	Yes
Is the event variance-based, threshold-based, or other?	Variance or threshold-based.
What are default values and units?	
Tolerance	92
Minimum threshold value	500M client payload bytes in 24 hours.
Maximum threshold value	1T downloaded payload bytes in 24 hours.
Is event tunable with non-variance-based parameters?	Yes
If so, what are its tunable attributes and units?	The event can be set to trigger off a particular number of bytes that does not take baselines or tolerance into account.

Questions about event	Response
Is event tunable outside of the normal policy editor	No
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	No
If so, what is it?	N/A

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The inside host that is sending the payload data.
What is the target?	The inside host or hosts that are receiving the payload data.
Which policy causes the event to trigger?	The source's policy.
What alarm categories does this security event contribute to for the source?	
In what quantity?	
What alarm categories does this security event contribute to for the target?	High Data Hoarding Index, High Target Index
In what quantity?	• High Data Hoarding Index: True • TI: True

What information is available in Secure Network Analytics?

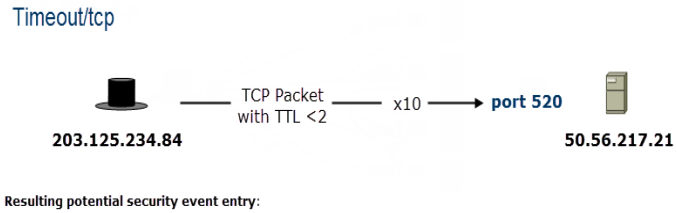
Questions about event	Response
What information is displayed in the alarm details?	Manager: Observed W bytes. Expected X bytes, tolerance of Y allows up to Z bytes. Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the target. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by target IP vs. Inside Hosts, the start time (reset hour) of the event's active day until the event’s last active time, server bytes greater than or equal to 1, and total bytes greater than or equal to 1k. Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_TARGET_DATA_HOARD (316)

Timeout/tcp

Mitigation is not available for the alarm associated with this security event.



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope Corporate	50.56.217.21	<CI value>*	Timeout/tcp-520(10)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	The source host has sent a TCP packet in which the TTL was less than 2. Because tracerouting occurs over UDP, TCP packets with short TTLs usually indicate malicious activity (i.e., firewalking) or a broken network (i.e., routing loops).
What does it mean when it triggers?	N/A
What are next steps?	N/A
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	For analyzing NetFlow, a FlowSensor is required.
Notes	none

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	
Which policies have this event on by default?	Inside Hosts, Outside Hosts
Which policies have this event off by default?	
Which policies have this alarm on by default?	
Which policies have this alarm off by default?	Inside Hosts, Outside Hosts
Can you tune this event?	No
Is the event variance-based, threshold-based, or other?	N/A
What are default values and units?	N/A
Tolerance	N/A
Minimum threshold value	N/A
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A

Questions about event	Response
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	
If so, what is it?	

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host that is the packet's source
What is the target?	The host that is the packet's destination
Which policy causes the event to trigger?	
What alarm categories does this security event contribute to for the source?	
In what quantity?	• High Recon Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	• TI: True

What information is available in Secure Network Analytics?

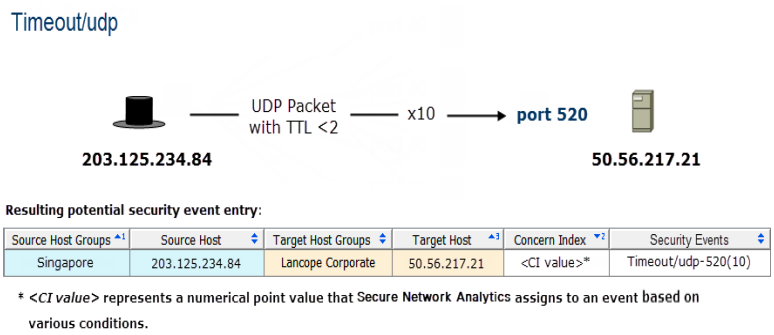
Questions about event	Response
What information is displayed in the alarm details?	Manager: View details. Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source & target IP, a time range five minutes before the event's first active time until the event's last active time, the associated port as <port>/TCP, and TCP. Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_TCP_TO (260)

Timeout/udp

Mitigation is not available for the alarm associated with this security event.



What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	The source host has sent a UDP packet in which the TTL was less than 2. Because tracerouting occurs over UDP, this security event can be fairly common; however, high numbers tend to imply a broken network (i.e., routing loops). Port 38293 is excluded from the UDP timeout to accommodate Norton Antivirus servers.
What does it mean when it triggers?	N/A
What are next steps?	N/A
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	To analyze NetFlow, you need a Flow Sensor.
Notes	None

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	
Which policies have this event on by default?	Inside Host, Outside Hosts
Which policies have this event off by default?	
Which policies have this alarm on by default?	
Which policies have this alarm off by default?	Inside Host, Outside Hosts
Can you tune this event?	No
Is the event variance-based, threshold-based, or other?	N/A
What are default values and units?	N/A
Tolerance	N/A
Minimum threshold value	N/A
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A

Questions about event	Response
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	
If so, what is it?	

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host that is the packet's source
What is the target?	The host that is the packet's destination
Which policy causes the event to trigger?	
What alarm categories does this security event contribute to for the source?	
In what quantity?	• High Recon Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	• TI: True

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: View details. Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source & target IP, a time range one minute before the event's first active time until the event's last active time, the associated port as <port>/UDP, and UDP. Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_UDP_TO (259)

Touched

The alarmed host (a host with a High Concern Index alarm or a Trapped Host security event) has initiated a connection with the target host and exchanged data.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	
In what quantity?	
What alarm categories does this security event contribute to for the target?	Attack Index, High Target Index
In what quantity?	• Attack Index: True • TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_TOUCHED (28)

Trapped Host

The host exceeded the accepted daily threshold of attempts to communicate with a host in a Trap host group on a port that is not in the configured services, which indicates potential “low and slow” scanning activity. The system performs these types of scans in order to prevent discovery of the attacker, the ports being scanned, or the hosts being scanned, or even to run a preliminary scan before the release of a worm.

Select the “Trap hosts that scan unused addresses in this group” check box on the Host Group Management page for a host group to enable the tracking of this type of activity for that particular host group. This is an advanced feature that you should enable only for specific, small, well-controlled host groups with fixed IP addresses and a stable number of hosts, such as critical servers. Doing so allows you to detect hosts intruding into the most important areas of your network.

Hosts that scan unused addresses in the Outside Hosts host group are not included in trapped host calculations and therefore do not generate trapped host alerts and alarms, regardless of whether this setting is enabled in the Outside Hosts host group.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	High Recon Index, High Concern Index
In what quantity?	• High Recon Index: True • CI: True
What alarm categories does this security event contribute	High Target Index

Questions about event	Response
to for the target?	
In what quantity?	• TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_TRAPPED_HOST (34)

UDP Flood

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	The source host has sent an excessive number of UDP packets in a 5-minute period. This may indicate a Denial of Service (DoS) attack or non-stealthy scanning activity.
What does it mean when it triggers?	This indicates that the source host is engaged in a DoS attack (potentially caused by either a compromised host or driven by a user), a misconfigured network application, or a connection with abnormally high UDP packets per second from the source. Many packets are often sent to consume a target's bandwidth as part of larger DDoS attacks. However, high UDP packet rates are more typical than high SYN packet rates, so a low threshold or tolerance setting may cause a high volume of false positives. Relatively low packet counts relative to a large amount of IPs is also likely to be a sign of reconnaissance.
What are next steps?	Determine how many UDP packets are being sent at what rate, when they were sent, and where they are going. An ideal way to investigate this is to perform a flow query for the source host. Set the start time of the query to five minutes before the start time of the associated security event, and set the end time to the end time of the alarm (if there is an alarm). Set the protocol filter to UDP only. Once the results have returned, find where the most UDP packets went during the searched time period. If the subject of the event is the client host in its UDP-

Questions about this event	Response
	heavy flows, you can sort on Client Packets or Client Packet Rate (pps). The goal is to find the standout flow (s). After finding the standout flow(s), determine whether or not this is expected behavior. Examples of expected behavior is a UDP-based VPN connection or uploads to a web server using UDP (like Google often does).
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	None
Notes	N/A

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	
Which policies have this event on by default?	Inside Hosts, Outside Hosts
Which policies have this event off by default?	
Which policies have this alarm on by default?	Inside Hosts, Outside Hosts
Which policies have this alarm off by default?	

Questions about event	Response
Can you tune this event?	Yes
Is the event variance-based, threshold-based, or other?	Both
What are default values and units?	N/A
Tolerance	75
Minimum threshold value	3.6k UDP Packets in 5 minutes
Maximum threshold value	10M UDP Packets in 5 minutes
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	
If so, what is it?	

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host sending UDP packets

Questions about event	Response
What is the target?	None
Which policy causes the event to trigger?	
What alarm categories does this security event contribute to for the source?	
In what quantity?	• High Ddos Source Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: Observed W pp5m. Expected X pp5m, tolerance of Y allows up to Z pp5m. Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source IP, a time range five minutes before the event's first active time until the event's last active time, and UDP. Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_UDP_FLOOD (6)

UDP Received

What is the security event?

Questions about this event	Response
What does it mean when it triggers?	This indicates that the target hosted is being targeted in a DoS attack, a misconfigured network application, or a connection with abnormally high UDP packets per second from the source(s). Many packets are often sent to consume a target's bandwidth as part of larger DDoS attacks. However, high UDP packet rates are more typical than high SYN packet rates, so a low threshold or tolerance setting may cause a high volume of false positives.
What are next steps?	The goal is to determine how many UDP packets are being received at what rate, when they were received, and where they are coming from. An ideal way to investigate this is to perform a flow query for the target host. Set the start time of the query to five minutes before the start time of the associated security event, and set the end time to the end time of the alarm (if there is an alarm). Set the protocol filter to *UDP only*. Once the results have returned, find where the most UDP packets came from during the searched time period. If the target of the event is the server host in its UDP-heavy flows, you can sort on either Client Packets or Client Packet Rate (pps). The goal is to find the standout flow(s). After finding the standout flow(s), determine whether or not this is expected behavior. An example of expected behavior is a UDP-based VPN connection.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	
In what quantity?	
What alarm categories does this security event contribute to for the target?	High Ddos Target Index, High Target Index
In what quantity?	• High Ddos Target Index: True • TI: True

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_UDP_RECEIVED (49)

Watch Host Active

What is the security event?

Questions about this event	Response
What does it mean when it triggers?	This is a user configured event that notifies you when a particular host is observed communicating. The meaning of the event can vary depending on why a user decided to put a particular host on the watch list, but it is generally a sign that any communication to or from the monitored host is inappropriate.
What are next steps?	The investigatory steps for this security event are entirely dependent on the context in which the host was added to the watch list.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	High Policy Violation Index, High Concern Index
In what quantity?	• High Policy Violation Index: True • CI: True
What alarm categories does	

Questions about event	Response
this security event contribute to for the target?	
In what quantity?	

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_WATCH_LIST (31)

Watch Port Active

What is the security event?

Questions about this event	Response
What does it mean when it triggers?	This is a user configured event that notifies you when a particular host is observed communicating over a particular port. The meaning of the event can vary depending on why a user decided to put a particular host on the watch list, but it is generally a sign that any communication to or from the monitored host is inappropriate.
What are next steps?	The investigatory steps for this security event are entirely dependent on the context in which the port was added to the watch list.

What policy settings are available for this security event?

Questions about event	Response
Is the event variance-based, threshold-based, or other?	

How does this security event contribute to categories?

Questions about event	Response
What alarm categories does this security event contribute to for the source?	High Policy Violation Index, High Concern Index
In what quantity?	• High Policy Violation Index: True • CI: True

Questions about event	Response
What alarm categories does this security event contribute to for the target?	
In what quantity?	

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_WATCH_PORT (13)

Worm Activity

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	The host has scanned and connected on a particular port across more than one subnet.
What does it mean when it triggers?	This security event indicates that a host appears to be performing an excess amount of reconnaissance across various internal networks, which may indicate that the host is compromised and attempting to propagate an infection throughout a network.
What are next steps?	This event can be noisy and its success largely depends on how well network scanners have been identified and placed into the network scanners host group. By doing this, these devices will inherit a policy that disables worm activity. Worm activity largely hinges upon a host scanning for similar ports across different logical /24 ranges. Begin by running a Top Ports (outbound) report. Set the time period to the day of the event and the client host to be the source IP of the event. Regardless of the target IP range that is listed, you can scan any type of host, so determine if you want to search on inside hosts, outside hosts, or both. On the Hosts tab in the Filter dialog, set the Server filter as appropriate, and on the Advanced tab, set the "Order the records returned by" to Flows. Sort the results by peers. Regardless, start at the top of the list as sorted by flows or peers to find the standout ports that either do not belong or appear abnormally high. Right-click an IP address to pivot to the flows to view the various IP addresses and determine if particular host groups are those being primarily targeted. You can also right- click and pivot to the Top Peers report to determine whether or not the traffic is

Questions about this event	Response
	spread generally equally across the targets. It is also worth noting the percentage of hosts that responded to the scans. At this point you should be able to determine who the host was scanning and what ports were being scanned.
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	
Notes	None

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	
Which policies have this event on by default?	Outside Hosts
Which policies have this event off by default?	
Which policies have this alarm on by default?	Outside Hosts
Which policies have this alarm off by default?	
Can you tune this event?	No
Is the event variance-based,	N/A

Questions about event	Response
threshold-based, or other?	
What are default values and units?	N/A
Tolerance	N/A
Minimum threshold value	N/A
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	
If so, what is it?	

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host that is the worm
What is the target?	The host that is the victim of the worm

Questions about event	Response
Which policy causes the event to trigger?	
What alarm categories does this security event contribute to for the source?	
In what quantity?	• Attack Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: Worm activity on port X ServiceName (Y Protocol). Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source & target IP, the start time (reset hour) of the event's active day until the event’s last active time, and the associated port as <port>/TCP & <port>/UDP. Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_WORM_ACTIVITY (35)

Worm Propagation

What is the security event?

Questions about this event	Response
What type of behavior is this event looking for?	The host has scanned and connected on a particular port across more than one subnet, and the host was previously scanned and connected to by a host for which the Worm Activity alarm has been triggerred.
What does it mean when it triggers?	This event seeks to find hosts that have been compromised by another compromised host, which results in the host attempting to compromise other hosts. This involves the following sequence of events: 1) A host is scanned by another host that is in the process of scanning multiple hosts; 2) The host that was just scanned now starts to scan other hosts.
What are next steps?	Run a Top Peers report on the host in question. Examine what other peer hosts contacted the subject on the specified port, filtering the report by the port in question. Verify that these hosts are not known scanners and should not have been participating in the observed scanning activity. If they are known scanners, the risk may be reduced. If they are not known scanners, the risk may increase since the scan was not legitimate or sanctioned. In this case, the event may indicate that the host is compromised.
Non-standard flow data required? (FlowSensor, proxy, firewall, etc.)	None
Notes	None

What policy settings are available for this security event?

Questions about event	Response
What policy settings are required for this security event to trigger?	
Which policies have this event on by default?	Inside Hosts, Outside Hosts
Which policies have this event off by default?	
Which policies have this alarm on by default?	Inside Hosts, Outside Hosts
Which policies have this alarm off by default?	
Can you tune this event?	No
Is the event variance-based, threshold-based, or other?	N/A
What are default values and units?	N/A
Tolerance	N/A
Minimum threshold value	N/A
Maximum threshold value	N/A
Is event tunable with non-variance-based parameters?	N/A
If so, what are its tunable attributes and units?	N/A

Questions about event	Response
Is event tunable outside of the normal policy editor	N/A
If so, what are the alternate locations of tunable values?	N/A
Does event have a default mitigation?	
If so, what is it?	

How does this security event contribute to categories?

Questions about event	Response
What is the source of the event?	The host that is the worm
What is the target?	The host that is the victim of the worm
Which policy causes the event to trigger?	
What alarm categories does this security event contribute to for the source?	
In what quantity?	• Attack Index: True • CI: True
What alarm categories does this security event contribute to for the target?	
In what quantity?	• TI: True

What information is available in Secure Network Analytics?

Questions about event	Response
What information is displayed in the alarm details?	Manager: Worm propagated X direction Source Host using Y ServiceName (Z Protocol). Desktop Client: N/A
What happens when you click the alarm details?	Manager: Displays the security events for the source host. Desktop Client: N/A
What information is shown for associated flows?	Manager: Flows are filtered by source & target IP, the start time (reset hour) of the event's active day until the event’s last active time, and client bytes & server bytes (both of which are greater than or equal to 1). Desktop Client: Flows are filtered by time period of last five minutes.

What information is available for responses for this security event?

Questions about event	Response
What is the event ID?	SEC_ID_WORM_PROPAGATION (36)

Alarm Categories

An alarm category is a “bucket” toward which a defined list of security events contributes index points (values that represent an observed occurrence of behavior that matches a defined set of criteria). When network activity meets or exceeds a defined set of criteria specified for this alarm category, it triggers an alarm. Each alarm category has its own list of security events that contribute index points to it and can cause it to generate alarms. Some security events contribute to more than one type of alarm category. A security event can also generate its own alarm, if configured to do so.

Alarm categories contain only host alarms. They do not contain the other four alarm types used in Secure Network Analytics, which are listed below.

- Manager system alarm
- Flow Collector system alarm
- Exporter or Interface alarm
- Host Group Relationship alarm

- For more information about these alarms, see the "Alarm List" topic in the Desktop Client Help.
- To configure settings for the alarms, use the Host Policy Manager in the Manager.

The following alarm categories are used. The tables below also indicate the index associated with an alarm category, the security events assigned to the alarm category, and the number of default points for each security event.

Anomaly

Tracks events that indicate that hosts are behaving abnormally or generating traffic that is unusual, but is not consistent with another category of activity.

The following security events are associated with the Anomaly alarm. The second column shows the number of default points assigned to the alarm category when the security event occurs. Some security events do not have points but are variables,

Name of Security Event	Number of Points Assigned to Category by Default
Connection from Bogon Address Attempted	900
Connection from Bogon Address Successful	14,400
Connection to Bogon Address Attempted	8,100
Connection to Bogon Address Successful	14,400
High Total Traffic	Based on observed estimated payload data.
High Traffic	Based on observed estimated payload data.
ICMP Frag Needed	700
ICMP Host Precedence	700
ICMP Host Unreach TOS	2,800
ICMP Net Unreach TOS	2,800
ICMP Precedence Cutoff	700
ICMP Proto Unreach	700
ICMP Src Route Failed	700
Low Traffic	3,000
Max Flows Initiated	Based on observed flow counters.
Max Flows Served	Based on observed flow counters.

Name of Security Event	Number of Points Assigned to Category by Default
New Flows Initiated	Based on observed flow counters.
Src=Des	4,000

Command & Control

Indicates the existence of bot-infected servers or hosts in your network attempting to contact a C&C server.

The following security events are associated with the C&C alarm: The second column shows the number of default points assigned to the alarm category when the security event occurs. Some security events do not have points but are variables.

Name of Security Event	Number of Points Assigned by Default
Beaconing Host	9,000
Bot Command And Control Server	32,000
Bot Infected Host - Attempted C&C Activity	22,400
Bot Infected Host - Successful C&C Activity	32,000
Fake Application Detected	4,000
Ping_Oversized_Packet	2,400
SSH Reverse Shell	11,700
Suspect Long Flow	4,000
Suspect Quiet Long Flow	4,000

Concern Index

Tracks hosts whose concern index has either exceeded the Concern Index (CI) threshold or rapidly increased.

Concern Index and Target Index categories use the same security events. If an event is triggered by a source host, it results in a Concern Index alarm. If an event is triggered by a target host, it results in a Target Index alarm.

The following security events are associated with the Concern Index alarm. The second column shows the number of default points assigned to the alarm category when the security event occurs. Some security events do not have points but are variables.

Name of Security Event	Number of Points Assigned by Default
Addr_Scan/TCP	4,000
Addr_Scan/UDP	4,800
Bad_Flag_ACK	4,800
Bad_Flag_All	4,800
Bad_Flag_NoFlg	4,800
Bad_Flag_Rsrvd	4,800
Bad_Flag_RST	4,800
Bad_Flag_SYN_FIN	4,800
Bad_Flag_URG	4,800
Beaconing Host	9,000
Bot Command and Control Server	32,000
Bot Infected Host – Attempted C&C Activity	22,400
Bot Infected Host – Successful C&C Activity	32,000

Name of Security Event	Number of Points Assigned by Default
Brute Force Login	10,800
Connection from Bogon Address Attempted	900
Connection from Bogon Address Successful	14,400
Connection from Tor Attempted	1,000
Connection from Tor Successful	4,000
Connection to Bogon Address Attempted	8,100
Connection to Bogon Address Successful	14,400
Connection to Tor Attempted	5,400
Connection to Tor Successful	5,400
Fake Application Detected	4,000
Flow Denied	162
Frag:First_Too_Short	6,000
Frag:Packet_Too_Long	6,000
Frag:Sizes_Differ	6,000
Half Open Attack	12,600
High File Sharing Index	Based on observed estimated payload data.
High SMB Peers	32,000
High Total Traffic	Based on observed estimated payload data.

Name of Security Event	Number of Points Assigned by Default
High Traffic	Based on observed estimated payload data.
High Volume Email	3,200
ICMP Flood	Based on observed ICMP packet counters.
ICMP_Comm_Admin	7
ICMP_Dest_Host_Admin	7
ICMP_Dest_Host_Unk	7
ICMP_Dest_Net_Admin	7
ICMP_Dest_Net_Unk	7
ICMP_Frag_Needed	700
ICMP_Host_Precedence	700
ICMP_Host_Unreach	7
ICMP_Host_Unreach_TOS	2,800
ICMP_Net_Unreach	7
ICMP_Net_Unreach_TOS	2,800
ICMP_Port_Unreach	7
ICMP_Precedence_Cutoff	700
ICMP_Proto_Unreach	700
ICMP_Src_Host_Isolated	7

Name of Security Event	Number of Points Assigned by Default
ICMP_Src_Route_Failed	700
ICMP_Timeout	1
Inside Tor Entry Detected	32,000
Inside Tor Exit Detected	32,000
Low Traffic	3,000
MAC Address Violation	6,300
Mail Rejects	2,400
Mail Relay	2,400
Max Flows Initiated	Based on observed flow counters.
New Flows Initiated	Based on observed flow counters.
New Host Active	2,800
Packet Flood	5,600
Ping	7
Ping_Oversized_Packet	2,400
Ping Scan	14,400
Port Scan	10,800
Reset/tcp	3
Reset/udp	2

Name of Security Event	Number of Points Assigned by Default
Scanner Talking	180
Slow Connection Flood	10,800
Spam Source	9,000
SSH Rev Shell	11,700
Stealth_Scan/tcp	5,200
Stealth_Scan/udp	4,800
Suspect Data Hoarding	Based on observed estimated payload data.
Suspect Data Loss	Based on observed estimated payload data.
Suspect Long Flow	4,000
Suspect Quiet Long Flow	4,000
Suspect UDP Activity	9,000
SYN Flood	Based on observed SYN flag counters.
Talks to Phantoms	1,440
Timeout/tcp	4
Timeout/udp	3
Trapped Host	11,700
UDP Flood	Based on observed UDP packet counters.

Name of Security Event	Number of Points Assigned by Default
Watch Host Active	32,000
Watch Port Active	32,000
Worm Activity	400
Worm Propagation	19,200

Data Hoarding

Indicates that a source or target host within a network has downloaded an unusual amount of data from one or more hosts.

The following security events are associated with the Data Hoarding alarm. The second column shows the number of default points assigned to the alarm category when the security event occurs. Some security events do not have points but are variables.

Name of Security Event	Number of Points Assigned by Default
Suspect Data Hoarding	Based on observed estimated payload data.
Target Data Hoarding	Based on observed estimated payload data.

DDoS Source

Indicates that a host has been identified as the source of a DDoS attack.

The following security events are associated with the DDoS Source alarm. The second column shows the number of default points assigned to the alarm category when the security event occurs. Some security events do not have points but are variables

Name of Security Event	Number of Points Assigned by Default
Half Open Attack	12,600
ICMP Flood	Based on observed ICMP packet counters.
Packet Flood	5,600
Slow Connection Flood	10,800
SYN Flood	Based on observed SYN flag counters.
UDP Flood	Based on observed UDP packet counters.

DDoS Target

Indicates that a host has been identified as the target of a DDoS attack.

The following security events are associated with the DDoS Target alarm The second column shows the number of default points assigned to the alarm category when the security event occurs. Some security events do not have points but are variables.

Name of Security Event	Number of Points Assigned by Default
Connection From Bogon Address Attempted	900
Connection From Bogon Address Successful	14,400
Half Open Attack	12,600
ICMP Received	Based on observed ICMP packet counters.
New Flows Served	Based on observed flow

Name of Security Event	Number of Points Assigned by Default
	counters.
Packet Flood	5,600
Slow Connection Flood	10,800
SYNs Received	Based on observed SYN flag counters.
UDP Received	Based on observed UDP packet counters.

Exfiltration

Tracks inside and outside hosts to which an abnormal amount of data has been transferred. If a host triggers a number of these events exceeding a configured threshold, it results in a Data Exfiltration alarm.

The following security events are associated with the Data Exfiltration alarm. The second column shows the number of default points assigned to the alarm category when the security event occurs. Some security events do not have points but are variables.

Name of Security Event	Number of Points Assigned by Default
Suspect Data Loss	Based on observed estimated payload data.

Exploitation

Tracks direct attempts by hosts to compromise each other, such as through worm propagation and brute force password cracking.

The following security events are associated with the Exploitation alarm The second column shows the number of default points assigned to the alarm category when the security event occurs. Some security events do not have points but are variables.

Name of Security Event	Number of Points Assigned by Default
Brute Force Login	10,800
Frag:First_Too_Short	6,000
Frag:Sizes_Differ	6,000
Frag:Packet_Too_Long	6,000
High SMB Peers	32,000
Scanner Talking	180
Suspect UDP Activity	9,000
Touched	8,000
Worm Activity	400
Worm Propagation	19,200

Policy Violation

The subject is exhibiting behavior that violates normal network policies.

The following security events are associated with the Policy Violation alarm. The second column shows the number of default points assigned to the alarm category when the security event occurs. Some security events do not have points but are variables.

Name of Security Event	Number of Points Assigned by Default
Connection from Tor Attempted	1,000
Connection from Tor Successful	4,000
Connection to Tor Attempted	5,400

Name of Security Event	Number of Points Assigned by Default
Connection to Tor Successful	5,400
High File Sharing Index	Based on observed estimated payload data.
High Volume Email	3,200
Inside Tor Entry Detected	32,000
Inside Tor Exit Detected	32,000
MAC Address Violation	6,300
Mail Rejects	2,400
Mail Relay	2,400
New Host Active	2,800
Spam Source	9,000
Watch Host Active	32,000
Watch Port Active	32,000

Recon

Indicates the presence of unauthorized and potentially malicious scans using TCP or UDP and being run against your organization's hosts. These scans, referred to as "reconnaissance," are early indicators of attacks against your network, and the scans may come from outside or inside your organization.

The following security events are associated with the Recon alarm. The second column shows the number of default points assigned to the alarm category when the security event occurs. Some security events do not have points but are variables.

Name of Security Event	Number of Points Assigned by Default
Addr_Scan/TCP	4,000
Addr_Scan/UDP	4,800
Bad_Flag_ACK	4,800
Bad_Flag_All	4,800
Bad_Flag_NoFlg	4,800
Bad_Flag_Rsrvd	4,800
Bad_Flag_RST	4,800
Bad_Flag_SYN_FIN	4,800
Bad_Flag_URG	4,800
Flow Denied	162
High SMB Peers	32,000
ICMP_Comm_Admin	7
ICMP_Dest_Host_Admin	7
ICMP_Dest_Host_Unk	7
ICMP_Dest_Net_Admin	7
ICMP_Dest_Net_Unk	7
ICMP_Host_Unreach	7
ICMP_Net_Unreach	7
ICMP_Port_Unreach	7

Name of Security Event	Number of Points Assigned by Default
ICMP_Src_Host_Isolated	7
ICMP_Timeout	1
Ping	7
Ping_Scan	14,400
Port Scan	10,800
Reset/tcp	3
Reset/udp	2
Stealth_Scan/tcp	5,200
Stealth_Scan/udp	4,800
Talks To Phantoms	1,440
Timeout/tcp	4
Timeout/udp	3
Trapped Host	11,700

Target Index

Tracks inside hosts that have been the recipient of more than an acceptable number of scan or other malicious attacks.

Concern Index and Target Index categories use the same security events. If an event is triggered by a source host, it results in a Concern Index alarm. If an event is triggered by a target host, it results in a Target Index alarm.

The following security events are associated with the Target Index alarm. The second column shows the number of default points assigned to the alarm category when the security event occurs. Some security events do not have points but are variables.

Name of Security Event	Number of Points Assigned by Default
Bad_Flag_ACK	4,800
Bad_Flag_All	4,800
Bad_Flag_NoFlg	4,800
Bad_Flag_Rsrvd	4,800
Bad_Flag_RST	4,800
Bad_Flag_SYN_FIN	4,800
Bad_Flag_URG	4,800
Beaconing Host	9,000
Bot Infected Host – Attempted C&C Activity	22,400
Bot Infected Host – Successful C&C Activity	32,000
Brute Force Login	10,800
Connection From Bogon Address Attempted	900
Connection From Bogon Address Successful	14,400
Connection From Tor Attempted	1,000
Connection From Tor Successful	4,000
Connection To Bogon Address Attempted	8,100
Connection To Bogon Address Successful	14,400
Fake Application Detected	4,000
Flow Denied	162

Name of Security Event	Number of Points Assigned by Default
Frag:First_Too_Short	6,000
Frag:Packet_Too_Long	6,000
Frag:Sizes_Differ	6,000
Half Open Attack	12,600
High SMB Peers	32,000
ICMP Received	Based on observed ICMP packet counters.
ICMP_Comm_Admin	7
ICMP_Dest_Host_Admin	7
ICMP_Dest_Host_Unk	7
ICMP_Dest_Net_Admin	7
ICMP_Dest_Net_Unk	7
ICMP_Frag_Needed	700
ICMP_Host_Precedence	700
ICMP_Host_Unreach	7
ICMP_Host_Unreach_TOS	2,800
ICMP_Net_Unreach	7
ICMP_Net_Unreach_TOS	2,800
ICMP_Port_Unreach	7

Name of Security Event	Number of Points Assigned by Default
ICMP_Precedence_Cutoff	700
ICMP_Proto_Unreach	700
ICMP_Src_Host_Isolated	7
ICMP_Src_Route_Failed	700
ICMP_Timeout	1
Inside Tor Entry Detected	32,000
Inside Tor Exit Detected	32,000
MAC Address Violation	6,300
Max Flows Served	Based on observed flow counters.
New Flows Served	Based on observed flow counters.
Packet Flood	5,600
Ping	7
Ping_Oversized_Packet	2,400
Port Scan	10,800
Reset/tcp	3
Reset/udp	2
Scanner Talking	180
Slow Connection Flood	10,800

Name of Security Event	Number of Points Assigned by Default
Src = Des	4,000
SSH Rev Shell	11,700
Stealth_Scan/tcp	5,200
Stealth_Scan/udp	4,800
Suspect Long Flow	4,000
Suspect Quiet Long Flow	4,000
Suspect UDP Activity	9,000
SYNs Received	Based on observed SYN flag counters.
Talks to phantoms	1,440
Target Data Hoarding	Based on observed estimated payload data.
Timeout/tcp	4
Timeout/udp	3
Touched	8,000
Trapped Host	11,700
UDP Received	Based on observed UDP packet counters.
Worm Propagation	19,200

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: http://www.cisco.com/c/en/us/support/index.html
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Change History

Document Version	Published Date	Description
1_0	August 15, 2024	Initial version.

Copyright Information